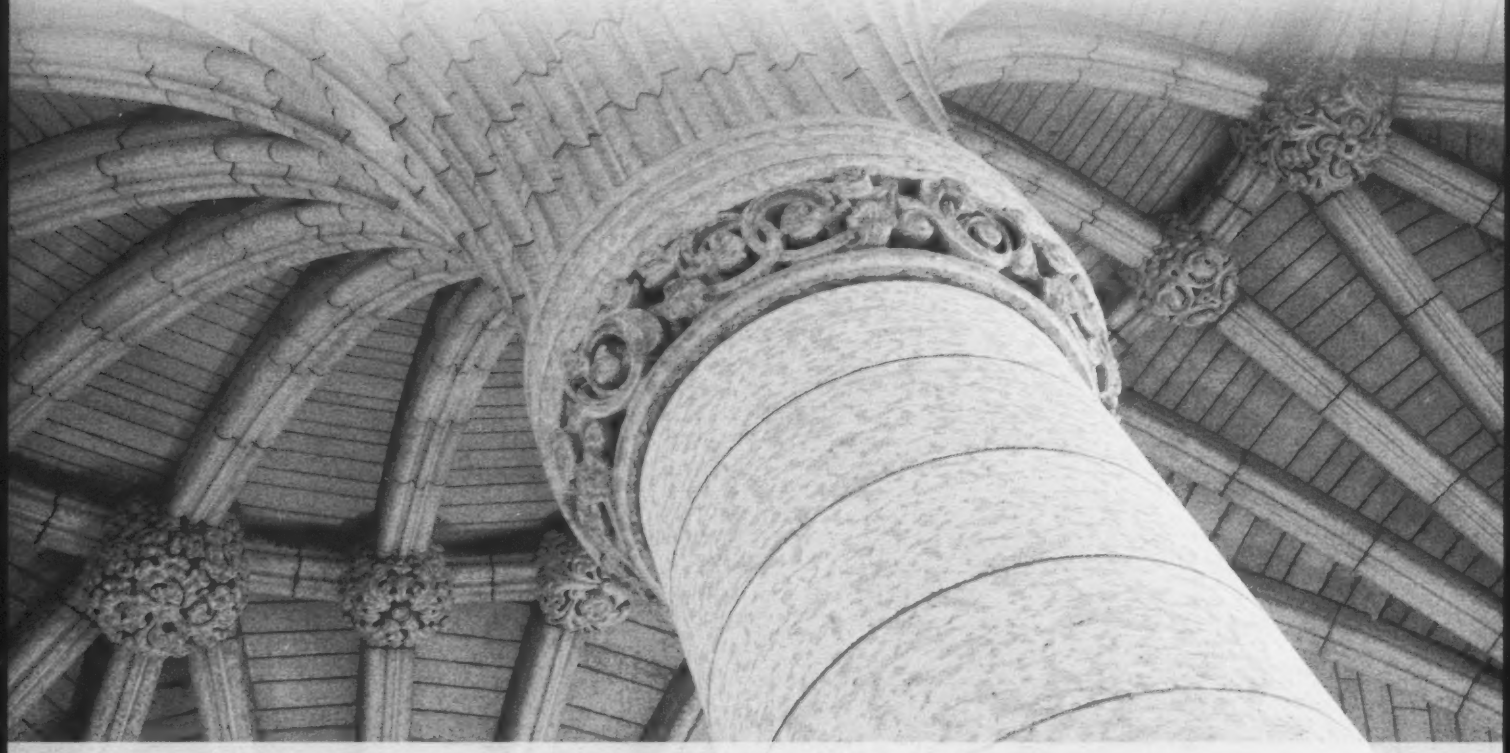
CHAMBRE DES COMMUNES
HOUSE OF COMMONS
CANADA

ABORDER LES VULNÉRABILITÉS DE LA VIE PRIVÉE NUMÉRIQUE ET LES MENACES POTENTIELLES AU PROCESSUS ÉLECTORAL DÉMOCRATIQUE CANADIEN

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Bob Zimmer, président



JUIN 2018
42e LÉGISLATURE, 1re SESSION

Publié en conformité de l'autorité du Président de la Chambre des communes

PERMISSION DU PRÉSIDENT

Les délibérations de la Chambre des communes et de ses comités sont mises à la disposition du public pour mieux le renseigner. La Chambre conserve néanmoins son privilège parlementaire de contrôler la publication et la diffusion des délibérations et elle possède tous les droits d'auteur sur celles-ci.

Il est permis de reproduire les délibérations de la Chambre et de ses comités, en tout ou en partie, sur n'importe quel support, pourvu que la reproduction soit exacte et qu'elle ne soit pas présentée comme version officielle. Il n'est toutefois pas permis de reproduire, de distribuer ou d'utiliser les délibérations à des fins commerciales visant la réalisation d'un profit financier. Toute reproduction ou utilisation non permise ou non formellement autorisée peut être considérée comme une violation du droit d'auteur aux termes de la *Loi sur le droit d'auteur*. Une autorisation formelle peut être obtenue sur présentation d'une demande écrite au Bureau du Président de la Chambre.

La reproduction conforme à la présente permission ne constitue pas une publication sous l'autorité de la Chambre. Le privilège absolu qui s'applique aux délibérations de la Chambre ne s'étend pas aux reproductions permises. Lorsqu'une reproduction comprend des mémoires présentés à un comité de la Chambre, il peut être nécessaire d'obtenir de leurs auteurs l'autorisation de les reproduire, conformément à la *Loi sur le droit d'auteur*.

La présente permission ne porte pas atteinte aux privilèges, pouvoirs, immunités et droits de la Chambre et de ses comités. Il est entendu que cette permission ne touche pas l'interdiction de contester ou de mettre en cause les délibérations de la Chambre devant les tribunaux ou autrement. La Chambre conserve le droit et le privilège de déclarer l'utilisateur coupable d'outrage au Parlement lorsque la reproduction ou l'utilisation n'est pas conforme à la présente permission.

Aussi disponible sur le site Web de la Chambre des communes à
l'adresse suivante : www.noscommunes.ca

ABORDER LES VULNÉRABILITÉS DE LA VIE PRIVÉE NUMÉRIQUE ET LES MENACES POTENTIELLES AU PROCESSUS ÉLECTORAL DÉMOCRATIQUE CANADIEN

Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Le président
Bob Zimmer

JUIN 2018

42e LÉGISLATURE, 1re SESSION

AVIS AU LECTEUR

Rapports de comités présentés à la Chambre des communes

C'est en déposant un rapport à la Chambre des communes qu'un comité rend publiques ses conclusions et recommandations sur un sujet particulier. Les rapports de fond portant sur une question particulière contiennent un sommaire des témoignages entendus, les recommandations formulées par le comité et les motifs à l'appui de ces recommandations.

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

PRÉSIDENT

Bob Zimmer

VICE-PRÉSIDENTS

Charlie Angus

Nathaniel Erskine-Smith

MEMBRES

Frank Baylis

Mona Fortier

Jacques Gourde

L'hon. Peter Kent

Joyce Murray*

Michel Picard

Raj Saini

Anita Vandenbeld

AUTRES DÉPUTÉS QUI ONT PARTICIPÉ

Ziad Aboultaif

L'hon. Maxime Bernier

Alexandre Boulerice

Kerry Diotte

Andy Fillmore

Michael Levitt

Wayne Long

Brian Masse

Kelly McCauley

Alistair MacGregor

Eva Nassif

Jean-Claude Poissant

Terry Sheehan

Marwan Tabbara

Mark Warawa

* Membre sans droit de vote, conformément à l'article 104(5) du Règlement.

GREFFIER DU COMITÉ

Jean-Denis Kusion

BIBLIOTHÈQUE DU PARLEMENT

Service d'information et de recherche parlementaires

Alexandra Savoie

Maxime-Olivier Thibodeau

LE COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

a l'honneur de présenter son

SEIZIÈME RAPPORT

Conformément au mandat que lui confère l'article 108(3)*h*)(vii) du Règlement et la motion adoptée le jeudi 22 mars 2018, le Comité a étudié l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook et a convenu de faire rapport de ce qui suit :

PRÉAMBULE

À la fin mars, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a entrepris une étude sur l'atteinte à la sécurité des renseignements personnels impliquant Cambridge Analytica et Facebook. L'étude s'étend également aux questions générales de la protection des renseignements personnels relativement aux monopoles de plateformes, qui occupent une place disproportionnée dans notre quotidien.

Le scandale a mis au jour des problèmes concernant la collecte massive de données, l'utilisation des données à des fins malicieuses et les menaces et les défis que représentent ces méthodes douteuses pour les démocraties partout dans le monde.

Selon les témoignages entendus à ce jour, le Comité s'inquiète gravement du fait que les processus démocratiques et électoraux du Canada soient également vulnérables à l'acquisition et à la manipulation inappropriées des données personnelles.

À la lumière des témoignages entendus, il apparaît clairement que le gouvernement du Canada doit agir de toute urgence afin d'assurer la protection de la vie privée des Canadiens. Il devrait :

- Renforcer les pouvoirs du Commissariat à la protection de la vie privée, notamment en donnant au commissaire à la protection de la vie privée le pouvoir d'imposer des sanctions importantes aux organisations qui ne respectent pas la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE);

- Assujettir les activités politiques aux lois qui assurent la protection des renseignements personnels des Canadiens;

- Encadrer les activités des organisations et des acteurs politiques de manière à assurer la transparence de la collecte, de l'utilisation et de la communication des renseignements personnels, y compris le recours à toute technique de ciblage et de profilage;

- Établir des règles et des exigences en matière de souveraineté des données de manière à assurer la protection des renseignements personnels des Canadiens;

- Mettre en œuvre les recommandations qu'a formulées le Comité dans son rapport sur la LPRPDE déposé en février 2018 afin d'harmoniser davantage les lois fédérales relatives à la protection des renseignements personnels avec le *Règlement général sur la protection des données* (RGPD) de l'Union européenne.

Le Comité est conscient qu'il n'a qu'effleuré la surface du problème dans son étude et que plusieurs autres conclusions devront être tirées. Il poursuivra son étude avec détermination, dans l'espoir de contribuer à une solution durable à un problème de portée mondiale.

Dans l'intervalle, le présent rapport provisoire présente les travaux du Comité et les témoignages qu'il a entendus au cours des premiers mois de son étude. Plus particulièrement, il présente plusieurs recommandations préliminaires au gouvernement du Canada.

TABLE DES MATIÈRES

LISTE DES RECOMMANDATIONS 1

ABORDER LES VULNÉRABILITÉS DE LA VIE PRIVÉE NUMÉRIQUE ET LES MENACES POTENTIELLES AU PROCESSUS ÉLECTORAL DÉMOCRATIQUE CANADIEN 5

INTRODUCTION 5

PARTIE 1 : L'ATTEINTE À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS 7

A. CONTEXTE 7

B. TÉMOIGNAGES DU DÉNONCIATEUR ET DES PARTIES CLÉS DE L'ATTEINTE À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS IMPLIQUANT CAMBRIDGE ANALYTICA ET FACEBOOK 7

1. Christopher Wylie 7

2. Chris Vickery 10

3. Facebook 14

4. AggregateIQ 19

PARTIE 2 : LE POINT DE VUE DE REPRÉSENTANTS D'ORGANISATIONS 22

A. MOZILLA CORPORATION 22

B. GOOGLE 24

C. CONSEIL DES INNOVATEURS CANADIENS 25

PARTIE 3 : LE POINT DE VUE DE COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE ET À L'INFORMATION ET D'UNIVERSITAIRES 28

A. ENQUÊTES EN COURS 28

1. Commissaire à la protection de la vie privée du Canada 28

2. Commissaire à l'information et la protection de la vie privée de la Colombie-Britannique 29

3. Commissaire à l'information du Royaume-Uni 29

B. COMMENTAIRES DES COMMISSAIRES À L'ÉGARD DE LEURS POUVOIRS D'EXÉCUTION 29

C. APPLICATION DE LA LÉGISLATION EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE AUX ACTIVITÉS POLITIQUES 35

CONCLUSION 41

Annexe A : Liste des témoins 43

Annexe B : Liste des mémoires 45

Procès-verbaux 47

Opinion dissidente du Parti conservateur du Canada et du Nouveau Parti démocratique du Canada 49

LISTE DES RECOMMANDATIONS

À l'issue de leurs délibérations, les comités peuvent faire des recommandations à la Chambre des communes ou au gouvernement et les inclure dans leurs rapports. Les recommandations relatives à la présente étude se trouvent énumérées ci-après.

Recommandation 1 sur la transparence :

Que le gouvernement du Canada établisse des exigences sur la transparence relativement à la collecte et à l'utilisation des données que font les organisations et les acteurs politiques, particulièrement au moyen des médias sociaux et d'autres plateformes en ligne afin de cibler la publicité politique ou autre à l'aide de techniques comme le profilage psycho-graphique. Ces exigences pourraient inclure, sans s'y limiter :

- **L'identification de la personne qui a payé pour la publicité, y compris la vérification de l'authenticité de la personne qui diffuse la publicité;**
- **L'identification du public cible et la raison pour laquelle le public cible a reçu la publicité; et**
- **L'enregistrement obligatoire concernant la publicité politique à l'extérieur du Canada. 10**

Recommandation 2 sur la mise en œuvre au Canada de mesures semblables à celles du *Règlement général sur la protection des données* :

Que le gouvernement du Canada mette immédiatement en œuvre des mesures pour veiller à ce que des protections semblables à celles du *Règlement général sur la protection des données* soient mises en place au Canada, y compris les recommandations contenues dans le rapport sur la *Loi sur la protection des renseignements personnels et les documents électroniques* présenté en février 2018..... 27

Recommandation 3 sur la souveraineté des données :

Que le gouvernement du Canada établisse des règles et des lignes directrices sur la propriété des données et la souveraineté des données afin de mettre un terme à la collecte et à l'utilisation non autorisées des renseignements personnels des citoyens. Ces règles et lignes directrices devraient tenir compte des défis que représente l'infonuagique. **27**

Recommandation 4 sur les pouvoirs d'exécution du commissaire à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir de rendre des ordonnances et le pouvoir d'imposer des amendes en cas de non-respect de ces ordonnances. **32**

Recommandation 5 sur les pouvoirs du commissaire à la protection de la vie privée en matière d'audit :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs étendus en matière d'audit, incluant le pouvoir de choisir les plaintes sur lesquelles enquêter. **33**

Recommandation 6 sur des pouvoirs d'exécution additionnels du commissaire à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir d'émettre des avis urgents à une organisation relativement à la production de documents pertinents dans une durée plus courte et le pouvoir de saisir des documents dans le cadre d'une enquête, sans préavis. **34**

Recommandation 7 sur le partage d'information entre le commissaire à la protection de la vie privée et d'autres organismes de régulation :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'autoriser le commissaire à la protection de la vie privée à partager certaines informations pertinentes dans le cadre d'enquêtes avec le Bureau de la concurrence, d'autres organismes de régulation canadiens et des organismes de régulation à l'échelle internationale, lorsque cela est approprié. 34

Recommandation 8 sur l'application des lois relatives à la protection de la vie privée aux activités politiques :

Que le gouvernement du Canada prenne certaines mesures afin d'assurer l'application de la législation en matière de protection de la vie privée aux activités politiques, soit par la modification des lois existantes ou par l'adoption d'une nouvelle loi. 41

ABORDER LES VULNÉRABILITÉS DE LA VIE PRIVÉE NUMÉRIQUE ET LES MENACES POTENTIELLES AU PROCESSUS ÉLECTORAL DÉMOCRATIQUE CANADIEN

INTRODUCTION

Le 22 mars 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (le Comité) a adopté une motion afin d'entreprendre une étude sur l'atteinte à la sécurité des renseignements personnels à laquelle sont associés Cambridge Analytica et Facebook[1]. La motion prévoit :

> Que, compte tenu de la vaste atteinte à la protection des données commise par Cambridge Analytica et de son non-signalement par Facebook pendant plusieurs années, le Comité étudie les répercussions sur la vie privée des monopoles de plateforme ainsi que les solutions législatives et réglementaires nationales et internationales possibles pour assurer la confidentialité des données des citoyens et l'intégrité des processus démocratiques et électoraux dans le monde, et qu'il entende notamment le témoignage du dénonciateur de Cambridge Analytica, Christopher Wylie, du commissaire à la protection de la vie privée du Canada, Daniel Therrien, et des administrateurs et des dirigeants de grandes entreprises de plateforme comme Facebook, Amazon et Google.

Jusqu'à maintenant, le Comité a tenu neuf réunions publiques sur ce sujet entre le 27 mars et le 12 juin 2018, au cours desquelles il a entendu un total de 16 témoins, dont certains ont comparu deux fois.

L'atteinte à la sécurité des renseignements personnels (l' « atteinte ») qu'a dévoilée Christopher Wylie (« M. Wylie » ou le «dénonciateur ») en exposant Cambridge Analytica, et par extension, Facebook, a créé dans les récents mois un engouement national et international envers l'importance de la protection des renseignements personnels et les risques liés à l'utilisation de tels renseignements afin d'influencer les processus démocratiques et électoraux.

---

1 Chambre des communes, Comité permanent de l'accès à l'information, de la protection des renseignements et de l'éthique (ETHI), *Procès-verbal*, 1re session, 42e législature, 22 mars 2018.

L'atteinte a incité le Comité à entreprendre la présente étude. Elle a également été intégrée à l'étude que mène le Comité spécial du numérique, de la culture, des médias et du sport du Royaume-Uni (le « Comité du numérique ») sur le phénomène des « fausses nouvelles »[2]. Aux États-Unis, elle a fait l'objet d'une audience commune devant le Comité sénatorial de la justice et le Comité sénatorial sur le commerce, la science et le transport, d'une audience devant le Comité des sciences et des transports de la Chambre des représentants, et d'une seconde audience devant le Comité sénatorial de la justice[3].

En raison de ce qui précède, le Comité tient à souligner le caractère exceptionnel de la présente étude. De par sa nature inter-juridictionnelle, le Comité se voit collaborer avec le Comité du numérique du Royaume-Uni, dont son président a d'ailleurs comparu devant lui[4]. Le Comité est également en communication avec ses collègues américains des Comités du Sénat et de la Chambre des représentants susmentionnés. Il a aussi entendu les témoignages de la commissaire à l'information du Royaume-Uni et du commissaire à l'information et la protection de la vie privée de la Colombie-Britannique. Ces interactions démontrent un effort sans précédent d'entraide mutuelle entre différentes juridictions devant l'ampleur du problème auxquels nous faisons face à l'ère des monopoles de plateformes technologiques et en raison de leur utilisation à des fins politiques malveillantes.

La présente étude soulève d'importantes questions relatives à l'intégrité des processus démocratiques et électoraux. Elle amène le Comité à se poser des questions à l'égard des mesures législatives qui pourraient être adoptées au Canada afin d'assurer une meilleure protection des renseignements personnels des Canadiens.

---

2 Comité du numérique, de la culture, des médias et du sport, Enquêtes, Parlement 2017, *Fake news.*

3 Comité sénatorial de la justice des États-Unis, Audiences, *Facebook, Social Media Privacy, and the Use and Abuse of Data*, 10 avril 2018 (cette audience était une audience commune avec le Comité sénatorial sur le commerce, la science et le transport); Comité de l'énergie et du commerce de la Chambre des représentants, Audiences, *Facebook: Transparency and Use of Consumer Data*, 11 avril 2018; Comité sénatorial de la justice des États-Unis, Audiences, *Cambridge Analytica and the Future of Data Privacy*, 16 mai 2018.

4 ETHI, *Témoignages*, 1re session, 42e législature, 3 mai 2018 (Damian Collins, président, Comité spécial du numérique, de la culture, des médias et du sport du Royaume-Uni).

PARTIE 1 : L'ATTEINTE À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS

A. CONTEXTE

Le 17 mars 2018, le *New York Times* et le journal britannique *The Guardian* ont tous deux publié un article portant sur l'entreprise Cambridge Analytica. L'histoire relatée dans ces deux publications repose sur les révélations du dénonciateur, M. Wylie, un ancien employé de Cambridge Analytica et de sa société mère : SCL Group (SCL). Elle révèle comment une atteinte à la sécurité des renseignements personnels perpétrée par Cambridge Analytica lui a permis de mettre la main sur plus de 87 millions de profils d'utilisateurs dans le monde, dont une grande proportion provenait des États-Unis[5]. Ce nombre a été confirmé par Facebook depuis[6]. Il est allégué que ces renseignements personnels ont été utilisés à des fins politiques malveillantes. L'atteinte a également permis d'obtenir les profils d'utilisateurs d'environ 620 000 citoyens canadiens[7].

B. TÉMOIGNAGES DU DÉNONCIATEUR ET DES PARTIES CLÉS DE L'ATTEINTE À LA SÉCURITÉ DES RENSEIGNEMENTS PERSONNELS IMPLIQUANT CAMBRIDGE ANALYTICA ET FACEBOOK

1. Christopher Wylie

M. Wylie a comparu devant le Comité le 29 mai 2018. Il a rappelé au Comité qu'il a été embauché en juillet 2013 par SCL et a quitté cette compagnie, qui à ce moment-là avait créé Cambridge Analytica, vers la fin de 2014[8]. M. Wylie a indiqué que c'est lui qui a communiqué avec Jeff Silvester et Zackary Massingham, afin de leur demander de travailler pour SCL et qu'AggregateIQ (AIQ) a été créée pour travailler sur des projets de SCL. Il a témoigné ne pas comprendre pourquoi AIQ nie avoir été créée pour travailler sur des projets du SCL (et éventuellement de Cambridge Analytica), alors que l'entreprise a été créée pour ce but spécifique[9].

---

5 *The New York Times*, « How Trump Consultants Exploited the Facebook Data of Millions », 17 mars 2018; *The Guardian*, « Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach », 17 mars 2018.

6 ETHI, *Témoignages*, 1re session, 42e législature, 19 avril 2018, 0900 (Kevin Chan, directeur mondial et chef des politiques publiques chez Facebook Canada, et Robert Sherman, chef adjoint de la protection des renseignements personnels, Facebook Inc.).

7 *Ibid.*

8 ETHI, *Témoignages*, 1re session, 42e législature, 29 mai 2018, 0850 (Christopher Wylie, dénonciateur).

9 *Ibid.*, 0915.

Bien qu'il soit d'accord que, sur papier, AIQ est une entreprise incorporée de façon séparée et entièrement canadienne, il maintient que l'entreprise agissait essentiellement comme si elle était une franchise de SCL[10]. M. Wylie a également été incrédule à l'idée qu'AIQ ait contribué à la création du programme Ripon sans avoir eu accès aux données qui alimentaient ce programme, indiquant ce qui suit : « Je ne vois pas comment on peut faire une recherche dans une base de données si on n'y a pas accès. Je ne sais pas comment vous pouvez faire du ciblage si vous n'avez pas accès à la base de données » [11].

M. Wylie a par ailleurs confirmé au Comité que lors d'une conversation qu'il a eue avec Jeff Silvester au printemps 2017, ce dernier lui aurait dit que ce qu'AIQ a fait dans le cadre du référendum sur le Brexit était « totalement illégal»[12]. M. Silvester nie avoir fait un tel commentaire[13].

M. Wylie a tenu à préciser que la collecte et l'utilisation de renseignements personnels n'implique pas toujours une intention malveillante ou contraire à l'éthique. Il est possible d'utiliser de tels renseignements et de distribuer des messages ciblés, sans pour autant que ce soit préjudiciable à ces personnes ou au processus démocratique (par exemple si les messages ciblés incitent les gens à aller voter alors qu'ils ne l'auraient pas fait autrement). Selon lui, les médias sociaux ne sont pas nécessairement néfastes. Ce sont des outils de travail. Il faut simplement imposer davantage de limites à l'utilisation qu'on peut en faire[14].

Pendant son témoignage, M. Wylie a proposé quelques solutions au Comité. Selon M. Wylie :

- Il serait bénéfique d'imposer aux entreprises canadiennes qui participent à des activités relatives à des campagnes politiques à l'extérieur du Canada de s'enregistrer auprès d'un organisme de régulation, comme le

---

10 *Ibid.*, 0945 et 0955.

11 Aleksandr Kogan est un professeur à l'Université Cambridge en Angleterre qui a créé une application sur Facebook consistant en un questionnaire comportant certaines questions personnelles. Cette application a permis de subtiliser les profils d'utilisateurs qui ont téléchargé l'application, mais aussi de tous leurs « amis Facebook », d'où le nombre de 87 millions d'utilisateurs dans le monde. La plateforme Ripon est un programme informatique créé par AIQ et utilisé par Cambridge Analytica dans le cadre de l'élection américaine de 2016, d'abord pour Ted Cruz, et ensuite pour Donald Trump. Il est allégué que les données recueillies et vendues par M. Kogan à Cambridge Analytica auraient été utilisées dans Ripon.

12 ETHI, *Témoignages*, 1re session, 42e législature, 29 mai 2018, 0950 (Christopher Wylie, dénonciateur).

13 ETHI, *Témoignages*, 1re session, 42e législature, 24 avril 2018, 0910 (Jeff Silvester, chef des opérations, AggregateIQ).

14 ETHI, *Témoignages*, 1re session, 42e législature, 29 mai 2018, 1025 (Christopher Wylie).

font par exemple les lobbyistes qui désirent travailler dans un pays étranger[15].

- Le gouvernement devrait procéder à une vérification plus diligente des projets antérieurs d'une entreprise avant de signer une entente contractuelle avec celle-ci (en vérifiant si dans les deux ans précédents elles ont participé à des projets internationaux contraires aux valeurs de promotion de la démocratie du Canada, par exemple)[16].

- Il devrait y avoir de meilleurs règlements imposant une plus grande transparence dans le domaine du ciblage, afin que les entreprises ou partis politiques qui affichent des messages ciblés soient redevables au public[17].

- Il devrait y avoir des règles à l'égard des attentes légitimes des gens relatives à l'utilisation des médias sociaux et leur consentement à l'égard de la collecte d'information par cette plateforme[18].

- Les législateurs de divers pays devraient collaborer ensemble afin de trouver une solution commune aux problèmes créés par la nature globale de l'Internet et de s'assurer que leurs démocraties demeurent intactes[19].

Sur ce dernier point, Damian Collins, le président du Comité du numérique, de la culture, des médias et du sport du Royaume-Uni, semble abonder dans le même sens. Il indique :

> [J]e crois qu'il est très important que nos comités collaborent et que les autorités de différents pays en fassent autant. Ces compagnies et ces enquêtes traversent plus d'une frontière. Je crois que pour réussir, nous devons être le plus intégrés possible[20].

---

15 *Ibid.*, 1015.

16 *Ibid.*

17 *Ibid.*, 1020 et 1025. Il suggère par exemple que Facebook et Google publient toutes les publicités qui sont envoyées à partir de leurs plateformes.

18 *Ibid.*, 1030 et 1035. Par exemple, si Facebook, a obtenu l'accès au contenu d'une page Facebook en 2008, qui est maintenant utilisé pour la reconnaissance faciale, est-ce que le consentement de l'utilisateur à avoir accès à son profil d'utilisateur est toujours valide?

19 *Ibid.*, 1050.

20 ETHI, *Témoignages*, 1re session, 42e législature, 3 mai 2018, 0920 (Damian Collins).

> Évidemment, différents pays mettront en place différentes règles, mais je suis certain que les règles relatives à la transparence seraient beaucoup plus efficaces si elles pouvaient être mises en application à l'échelle internationale.[21].

À la lumière de ces renseignements, le Comité recommande :

Recommandation 1 sur la transparence :

Que le gouvernement du Canada établisse des exigences sur la transparence relativement à la collecte et à l'utilisation des données que font les organisations et les acteurs politiques, particulièrement au moyen des médias sociaux et d'autres plateformes en ligne afin de cibler la publicité politique ou autre à l'aide de techniques comme le profilage psycho-graphique. Ces exigences pourraient inclure, sans s'y limiter :

- **L'identification de la personne qui a payé pour la publicité, y compris la vérification de l'authenticité de la personne qui diffuse la publicité;**
- **L'identification du public cible et la raison pour laquelle le public cible a reçu la publicité; et**
- **L'enregistrement obligatoire concernant la publicité politique à l'extérieur du Canada.**

2. Chris Vickery

Chris Vickery, un expert en sécurité des données, a expliqué lors de sa comparution devant le Comité le 17 avril 2018 que son travail consiste principalement à traquer les fuites de données :

> Au cours des dernières années, je me suis taillé une réputation de grand expert sur la prévalence et les causes des fuites de données, de même que sur les modèles d'intervention communs des entités touchées. Je vous prie de noter toutefois que les fuites de données que je localise et sécurise ne sont pas le fait d'actions malveillantes ou d'exploitation des ordinateurs. Il s'agit tout simplement de données qui, pour une raison ou une autre, se promènent à l'air libre, et dont personne ne s'est rendu compte jusqu'à ce que j'intervienne. Et vous seriez surpris du nombre de fois où cela se produit. Il y a une épidémie d'erreurs de configuration sur Internet[22].

---

21 *Ibid.*, 1015.

22 ETHI, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0850 (Chris Vickery, directeur de la recherche sur les risques cybernétiques, UpGuard, à titre personnel).

Il a mentionné avoir notamment sécurisé des fuites de données en provenance des entreprises Verizon, Viacom, Microsoft et Hewlett-Packard, du département de la Défense des États-Unis, de l'institut national électoral au Mexique (l'INE), ainsi que du site Web de Donald Trump lors de la campagne présidentielle de 2016[23].

En ce qui concerne AIQ, M. Vickery a expliqué qu'il en a appris l'existence le 20 mars 2018 en consultant un site Web ouvert au public appelé GitHub où les développeurs collaborent et publient un code source ouvert[24].

> J'ai vu un renvoi à @aggregateiq.com au sujet d'un code de SCL Group qui était à l'air libre et accessible au public. J'ai suivi les miettes de pain, découvert qui était AggregateIQ et remarqué que l'entreprise avait un sous-domaine appelé GitLab. Quand j'ai regardé gitlab.aggregateiq.com, je me suis rendu compte qu'on pouvait s'inscrire et, qu'en fait, l'entreprise invitait toute la planète à s'ouvrir un compte sur son portail de collaboration.
>
> Je me suis donc ouvert un compte, je suis entré sur le site, et j'ai eu accès à tous les outils, utilitaires, authentifiants, messages, problèmes et notes des employés, et les demandes de fusion me sont apparues. Je me suis vite rendu compte de l'importance de cela et que cela intéresserait au plus haut point les organismes de réglementation, les gouvernements et les gens de plusieurs pays, alors j'ai commencé le téléchargement. Normalement, je m'efforce de protéger les gens qui peuvent être touchés par ce genre de choses, mais je dois dire que, dans ce cas, l'intérêt évident de la population de connaître la vérité au sujet des activités de Cambridge Analytica, AggregateIQ et SCL Group a été un facteur décisif[25].

Selon M. Vickery, certaines questions sont toujours sans réponse dans ce dossier. En effet, il a confié au Comité que « [m]ême si j'examine encore une partie des données, je n'ai pas encore compris exactement les liens d'AggregateIQ avec SCL Group et Cambridge Analytica. Les murs qui séparent ces entités sont très poreux »[26]. Selon lui, il est clair que les trois entités ont eu accès aux permissions d'accès et aux données[27].

Une autre question qui mérite l'attention du Comité, selon M. Vickery, est de savoir dans quelle mesure, si c'est le cas, AIQ ou ses employés ont utilisé des renseignements privés ou politiques à accès limité à des fins commerciales et lucratives. Il a déclaré ce qui suit :

---

23 *Ibid.*

24 *Ibid.*, 0850 et 0855.

25 *Ibid.*

26 *Ibid.*, 0855.

27 *Ibid.*

> J'ai trouvé des preuves de la présence de réseaux de publicité en formation sous le même domaine, dont un qui s'appelle notamment Ad*Reach [...], de même que aq-reach. Un des employés qui travaillait à AIQ travaillait aussi pour une entreprise de publicité appelée easyAd Group AG, basée en Suisse et ayant des filiales aux États-Unis et en Russie. J'adorerais savoir quel genre de travail on faisait et si les données qui transitaient par AIQ étaient utilisées dans ces campagnes de publicité ou ces montages sur lesquels travaillait l'employé à ce moment[28].

M. Vickery a également attiré l'attention des membres du Comité sur un projet de cryptomonnaie qui se trouve dans le dépôt de données d'AIQ qu'il a trouvé en ligne, appelé Midas, dans lequel le site Web concerné vendait la cryptomonnaie pour un montant minimal de 10 000 $[29]. D'après M. Vickery,

> Le site Web a été fermé depuis que l'affaire a été rendue publique, et si vous voulez mon avis, il y a anguille sous roche. Si vous pouviez découvrir pourquoi quelqu'un tentait de concevoir une cryptomonnaie sur AggregateIQ GitLab, pour vente au public, et pourquoi on voulait le faire à l'abri des regards, je pense que cela vaudrait la peine d'enquêter[30].

Jeff Silvester, le chef des opérations d'AIQ, a dit au Comité que le projet de crypto-monnaie était en préparation pour un client de la Colombie-Britannique et que ce projet n'a pas encore été lancé[31].

En réponse aux questions des membres du Comité, M. Vickery a expliqué que, dans sa documentation, AIQ décrit en détail son système pour amalgamer différentes bases de données. Ce système, dans lequel Facebook joue un rôle, est le suivant :

> Au départ, elles sont amalgamées par l'entrepôt de données du Data Trust du RNC, soit le Republican National Committee ici aux États-Unis. J'avais trouvé la base de données du Data Trust avant qu'elle fasse partie des résultats de recherche en juin 2017. Elle est assez étendue. Elle contient des données fusionnées avec i360, qui est une entreprise spécialisée dans les renseignements politiques financée par les frères Koch. Data Trust a supprimé un article de blogue dans lequel il faisait valoir que ses données avaient été fusionnées avec celles d'i360.
>
> Il y a aussi L2 Political. Cette entreprise a fourni des données à cette énorme machine. Cambridge Analytica l'a récemment admis sur son site Web.

---

28 *Ibid.*

29 *Ibid.*, 0900.

30 *Ibid.*

31 ETHI, *Témoignages*, 1re session, 42e législature, 24 avril 2018, 0905 (Jeff Silvester).

> Il est évident que Facebook entre en ligne de compte. La documentation d'AggregateIQ explique ensuite que les bases de données commerciales sont visées. Je sais qu'Experian en est une qui a versé des données au dossier du Deep Root Analytics du RNC que j'ai trouvé en 2017. Si je le sais, c'est qu'il y avait des identifications d'Experian pour chaque identification d'électeur et que les habitudes de consommation de chaque personne y étaient associées.
>
> AggregateIQ affirme aussi que les candidats peuvent apporter leurs propres sources d'information concernant les bénévoles, les partisans et les donateurs. Ils réunissent toutes ces données dans une « base de données de la vérité » principale, comme ils l'appellent. Les registres électoraux de l'État corroborent ensuite le contenu des dossiers du RNC.
>
> Alors, il n'y a vraiment aucune limite à ce qu'ils peuvent y ajouter[32].

M. Vickery a également expliqué que SCL et AIQ semblent travailler avec la même base de codes, malgré le fait que les représentants d'AIQ affirment que les deux entreprises n'ont aucun lien entre elles[33]. Aussi, la base de codes contient un champ « client » où il était écrit « Cambridge Analytica », selon ce que M. Vickery a découvert.

> Je ne vois pas pourquoi le SCL Group dirait que Cambridge Analytica est un de ses clients puisqu'il est, au fond, propriétaire de Cambridge Analytica. Le SCL Group est son organisation mère. La seule explication raisonnable pour moi est que ce serait AggregateIQ qui aurait indiqué que Cambridge Analytica était son client, avant de transmettre le code au SCL Group, code qui n'aurait pas été modifié immédiatement. Il y a là une petite situation triangulaire[34].

M. Vickery a rappelé que dans ses déclarations publiques récentes, Cambridge Analytica a présenté des exemples de données qu'elle a utilisées, et à indiquer un lien potentiel avec la documentation d'AIQ.

> Récemment, je suppose qu'elle s'est sentie obligée d'être transparente quant à l'origine des données. Elle a avoué qu'elle avait les données du Data Trust du RNC. Les identifications du RNC se trouvent partout dans les champs, les catégories, les scripts cibles et les analyseurs qui se trouvent dans le dépôt central d'AggregateIQ ainsi que dans sa documentation. Donc, si les données [sont transférées] directement de l'un à l'autre, il est clair qu'ils traitent le même type de données[35].

---

32 *Ibid.*, 0905.

33 *Ibid.*, 0930.

34 *Ibid.*, 0910.

35 *Ibid.* En raison de difficultés techniques lors de l'enregistrement du témoignage, le Comité a déduit que les mots « sont transférées» manquent dans cette citation.

Dans le but d'illustrer la manière dont l'argent a circulé entre Cambridge Analytica et AIQ, M. Vickery a fourni l'exemple de la plateforme Ripon, utilisée pour la campagne présidentielle de Ted Cruz en 2016 :

> L'équipe de Ted Cruz croyait que l'argent qu'elle payait pour ce produit – sa mise au point, le service connexe, etc. – allait à Cambridge Analytica, alors que c'est AggregateIQ qui travaillait là-dessus. C'est AggregateIQ qui faisait tout le travail, mais les chèques, eux, étaient adressés à Cambridge Analytica[36].

M. Vickery a expliqué qu'il voit AIQ comme une division d'une plus grande entité, et l'a comparée « au département de développement d'une grande entreprise »[37]. Selon lui, il est probable que la grande entreprise en question soit SCL, les objectifs et les résultats finaux des deux entités étant parallèles[38].

Enfin, en ce qui concerne Facebook, M. Vickery a constaté que l'utilisation et l'exploitation potentielle d'applications offertes sur Facebook étaient un problème très répandu. Il a découvert que l'une des applications de Facebook liées à AIQ (le nom d'AIQ figure sur l'application à titre de racleur) a été classée dans la catégorie « Jeux » des applications de Facebook[39]. AIQ a été suspendue de la plateforme Facebook, mais selon M. Vickery, l'identificateur de l'application en question figure toujours dans le code qu'il a trouvé[40].

M. Vickery a comparu devant le Comité une deuxième fois le 7 juin 2018 pour répondre à de nouvelles questions et pour fournir des détails supplémentaires concernant sa découverte du dépôt de données d'AIQ. Le Comité tient à souligner l'apport du témoignage de M. Vickery et l'utilité de son analyse technique, qui a permis au Comité de mieux saisir les tenants et aboutissants de l'atteinte aux données qui fait l'objet de son étude.

3. Facebook

Kevin Chan, directeur mondial et chef de la politique publique pour Facebook Canada, et Robert Sherman, directeur adjoint de la protection des renseignements personnels pour Facebook, ont comparu devant le Comité au nom de Facebook. Tout en précisant que

---

36 *Ibid.*, 0930.

37 *Ibid.*, 1030.

38 *Ibid.*

39 *Ibid.*, 1005.

40 *Ibid.*

Facebook ne connaissait pas encore tous les faits concernant Cambridge Analytica, M. Chan a qualifié la situation d' « énorme abus de confiance » envers les utilisateurs de Facebook[41].

Les représentants de Facebook ont reconnu que les erreurs suivantes ont été commises par l'entreprise :

- Facebook n'a pas investi assez dans la sécurité de sa plateforme et elle en est responsable[42];
- Facebook n'en a pas fait assez pour empêcher que les outils puissants acquis par ses utilisateurs ne soient utilisés à des fins préjudiciables[43];
- Facebook n'a pas adopté une vision assez large de sa responsabilité[44];
- « Nous reconnaissons que, par le passé, nous nous sommes montrés trop idéalistes quant à l'utilisation de nos technologies et que nous ne nous sommes pas suffisamment concentrés sur la prévention des abus sur notre plateforme[45] »;
- Facebook aurait dû aviser les utilisateurs concernés par l'affaire Cambridge Analytica dès 2016[46];
- La façon dont fonctionnait la plateforme de Facebook, avant certains changements apportés en 2014 pour limiter l'information que les développeurs d'applications peuvent recueillir, « n'est pas la bonne façon de fonctionner pour une plateforme[47] »;

---

41 ETHI, *Témoignages*, 1re session, 42e législature, 19 avril 2018, 0850 (Kevin Chan, directeur mondial et chef de la politique publique, Facebook Canada, Facebook Inc.).

42 *Ibid.*

43 *Ibid.*

44 *Ibid.*

45 *Ibid.*, 0855.

46 *Ibid.*, 0900 (Robert Sherman, directeur adjoint de la protection des renseignements personnels, Facebook Inc.).

47 *Ibid.*

- Facebook a été trop lente à déceler les menaces d'ingérence étrangère au moyen de faux comptes et de désinformation lors des dernières élections présidentielles aux États-Unis[48].

Le Comité est particulièrement troublé par le fait que Facebook ait reconnu que des messages privés ont pu être partagés sans le consentement des utilisateurs concernés, étant donné les attentes élevées en matière de protection de la vie privée associées à ce genre de communication[49].

Les représentants de Facebook ont souligné que l'entreprise avait déjà pris – ou avait l'intention de prendre – les mesures suivantes afin de résoudre les problèmes identifiés :

- La semaine précédant le témoignage de ses représentants devant le Comité, Facebook a commencé à présenter à tous ses utilisateurs la liste des applications qu'ils ont utilisées en même temps qu'une façon de révoquer les permissions accordées à ces applications par le passé (ce qui constitue un rappel de ce que les utilisateurs peuvent déjà faire dans leurs paramètres de protection de la vie privée)[50];

- En réponse au rapport du Centre de la sécurité des télécommunications du Canada publié en 2017 qui mentionne deux domaines où Facebook a un rôle à jouer, soit la cybersécurité et le piratage des comptes en ligne des candidats et des partis politiques, ainsi que la diffusion de désinformation en ligne, Facebook a lancé à l'automne 2017 une « initiative canadienne sur l'intégrité des élections », qui comporte cinq éléments :

  - un « Guide d'hygiène informatique » destiné aux politiciens et aux partis politiques canadiens;

  - une formation en « hygiène informatique » offerte aux partis politiques fédéraux;

  - une ligne de courriel sur les cybermenaces destinée aux politiciens et aux partis politiques canadiens;

---

48 *Ibid.*, 1005 (Kevin Chan).

49 *Ibid.*, 1035 (Robert Sherman).

50 *Ibid.*, 0850 (Robert Sherman).

- un partenariat avec HabiloMédias, le Centre canadien d'éducation aux médias et de littératie numérique, établi pour lutter contre la désinformation en ligne;

- un « test de transparence de la publicité », appelé « View Ads », qui a été lancé au Canada en novembre 2017 et qui permet à un utilisateur de Facebook au Canada de voir toutes les annonces Facebook, y compris celles pour lesquelles l'utilisateur en question ne fait pas partie de l'auditoire visé[51].

- Facebook est en train d'informer les utilisateurs de Facebook au Canada – et ailleurs dans le monde – s'ils sont touchés par l'affaire Cambridge Analytica au moyen de messages apparaissant au haut de leur fil de nouvelles Facebook, où il sera mentionné que les utilisateurs peuvent accéder à l'information sur les applications qui ont recueilli leurs renseignements personnels[52];

- En ce qui concerne les développeurs d'applications associés à Facebook et les autres tierces parties avec lesquelles Facebook a des relations d'affaires (dans la catégorie d'Aleksandr Kogan, par exemple) Facebook devra « investir massivement dans du personnel et des processus supplémentaires pour nous assurer d'avoir une surveillance dans ces domaines[53] »;

- Facebook, et la société en général, devrait investir davantage dans les moyens de communiquer avec les individus au sujet de la protection des renseignements personnels[54];

- Les mesures de contrôle annoncées récemment par Facebook permettent aux utilisateurs de consulter une seule carte centralisée où ils ont un contrôle total sur leur expérience et leur vie privée sur Facebook, alors qu'auparavant ils devaient parfois passer par 20 écrans différents pour arriver au même résultat[55];

---

51 *Ibid.*, 0855 (Kevin Chan).

52 *Ibid.*, 0900 (Robert Sherman).

53 *Ibid.*, 0945.

54 *Ibid.*, 0950.

55 *Ibid.*, 0855(Kevin Chan).

- Facebook a mis en place des outils d'intelligence artificielle pour lui permettre de supprimer, avant que le méfait se produise, les faux comptes utilisés pour s'ingérer dans des élections[56];

- Concernant la publicité politique pour les élections de mi-mandat aux États-Unis, Facebook prendra des mesures supplémentaires pour s'assurer de l'authenticité de la personne qui gère les comptes publicitaires concernés[57];

- En ce qui a trait au problème de prélèvement à grande échelle d'information publique généralement disponible sur Internet, appelé le « scraping », auquel Facebook – et tous les services Internet – est aux prises, Facebook a mis en place des mesures techniques pour régler ce problème et déterminer quand il se produit[58].

M. Sherman a mentionné que Facebook a mis en place une série de restrictions sur la façon dont les développeurs d'applications peuvent utiliser l'information de la plateforme :

> y compris le fait qu'ils ne peuvent pas demander de l'information dont ils n'ont pas besoin pour faire fonctionner leurs applications. Ils ne peuvent pas vendre l'information qu'ils reçoivent. Ils ne peuvent pas l'utiliser aux fins de monétisation, de réseaux d'applications ou ce genre de choses. Ils doivent supprimer l'information si nous ou quelqu'un d'autre leur demandons de le faire[59].

En ce qui concerne l'entrée en vigueur du *Règlement général sur la protection des données* (RGPD) dans l'Union européenne et de son application, M. Sherman a affirmé, en réponse aux questions des membres du Comité, que

> Dans le cadre de notre travail préparatoire en vue de l'adoption du Règlement général de l'Union européenne, nous avons mis en place de nouveaux paramètres de contrôle de la protection des données personnelles ainsi que d'autres mesures et nous avons l'intention de déployer ces mesures au Canada également[60].

Enfin, les représentants de Facebook se sont engagés à faire un suivi avec le Comité et de lui fournir une liste de tous les genres de renseignements personnels qui auraient été

---

56 *Ibid.*, 1010.

57 *Ibid.*, 1030.

58 *Ibid.*, 1040.

59 *Ibid.*, 1025.

60 *Ibid.*, 0915.

communiqués sans le consentement des utilisateurs, ainsi que le résultat obtenu après avoir fait le rapprochement entre le nombre d'applications qui ont partagé des informations personnelles sans le consentement des utilisateurs et le nombre d'utilisateurs touchés[61]. Au moment de la publication du présent rapport, Facebook n'avait pas encore fourni l'information demandée.

Le Comité s'assurera du suivi de Facebook et espère que, lorsque Facebook aura terminé son enquête interne concernant Cambridge Analytica et que tous les faits pertinents seront connus, sa réaction sera dans la même mesure que le problème qui a été mis au jour.

4. AggregateIQ

Forts des renseignements fournis, notamment, par M. Vickery, les membres du Comité ont cherché à mieux comprendre le rôle d'AIQ dans l'atteinte aux données concernant Facebook et Cambridge Analytica. Zackary Massingham, directeur général, et Jeff Silvester, chef des opérations, ont comparu au nom d'AIQ le 24 avril 2018. M. Massingham a affirmé qu'AIQ n'est pas, et n'a jamais été, un segment ou une filiale de SCL ou de Cambridge Analytica et qu'elle est entièrement canadienne[62]. Il a aussi affirmé que tout le travail que fait AIQ pour ses clients demeure distinct, sans relation avec les services offerts à d'autres clients et que les seuls renseignements personnels qu'ils utilisent dans leur travail sont ceux fournis par leurs clients[63]. Selon M. Massingham, AIQ n'a « jamais puisé, géré, ni utilisé des données Facebook qui auraient été obtenues de façon irrégulière par Cambridge Analytica ou par quiconque[64] ».

M. Silvester a ajouté ce qui suit à la description du travail effectué par AIQ :

> Nous ne sommes pas une société de mégadonnées. Nous ne sommes pas une entreprise d'analyse de données. Nous ne recueillons pas des données illégalement. Nous ne divulguons jamais l'information d'un client à un autre, et nous n'exerçons pas ce qu'on appelle les arts obscurs du numérique. Comme Zack l'a dit, nous faisons de la publicité en ligne et nous créons des sites Web et des logiciels pour nos clients[65].

Il a également mentionné que Facebook et Google leur fournissent toute l'information dont ils ont besoin pour cibler un public :

---

61 *Ibid.*, 1040.

62 ETHI, *Témoignages*, 1re session, 42e législature, 24 avril 2018, 0845 (Zackary Massingham).

63 *Ibid.*

64 *Ibid.*

65 *Ibid.* (Jeff Silvester).

> Avec Facebook, en particulier, nous pouvons cibler des gens en fonction de leur lieu géographique, jusqu'au niveau de leur code postal. Nous pouvons faire du ciblage publicitaire en fonction de caractéristiques démographiques générales, comme le sexe ou le groupe d'âge et aussi en fonction des domaines d'intérêt. C'est vraiment tout ce dont nous avons besoin pour bâtir une campagne publicitaire et ces données nous sont fournies par le client[66].

M. Silvester a expliqué la présence de renseignements personnels dans le répertoire de codes d'AIQ comme découlant d'une erreur de leur part : « Ils n'étaient pas censés être là, et vous m'en voyez désolé, comme le responsable ultime que je suis[67]. »

Le Comité n'adhère pas à la version des faits que lui a présentée les représentants d'AIQ parce que, d'une part, leur témoignage est inconstant et parsemé de contradictions et que, d'autre part, il va à l'encontre du témoignage de plusieurs témoins crédibles. Par exemple, M. Massingham affirme qu'AIQ n'a aucun lien avec SCL, alors que son nom apparait dans certains documents en tant que dirigeant de SCL Canada et que SCL avait inscrit que sa ligne téléphonique directe correspondait au numéro de SCL Canada[68]. Sur ce dernier point, M. Massingham a affirmé qu'il a seulement réalisé que c'était le cas lorsque l'histoire est sortie dans les médias[69]. M. Massingham et M. Silvester ont tous deux nié qu'AIQ se soit déjà affichée comme étant SCL Canada ou que SCL Canada, comme entité distincte, ait déjà existée[70].

Concernant le travail exécuté par AIQ pour la campagne en faveur du retrait du Royaume-Uni de l'Union européenne, le Brexit, M. Silvester a déclaré n'être au courant d'aucune coordination entre les quatre clients d'AIQ impliqués dans cette campagne (DUP, BeLeave, Vote Leave et Veterans for Britain)[71].

À cet égard, M. Massingham a déclaré qu'il n'était même pas au courant qu'il y avait un lecteur BeLeave au sein de celui de Vote Leave[72]. M. Silvester a ensuite corrigé M. Massingham en disant :

> Permettez-moi de préciser que nous avions accès au lecteur de Vote Leave [...] Le lecteur en soi était un lecteur Vote Leave, et des images étaient sur ce lecteur. Nous

---

66 *Ibid.*, 0955.

67 *Ibid.*, 0845.

68 *Ibid.*, 1010 .

69 *Ibid.*

70 *Ibid.*, 0905, 0910, 1005 et 1010 (Zackary Massingham); *Ibid.*, 0910, 0930, 1010 et 1035 (Jeff Silvester).

71 *Ibid.*, 0855 (Jeff Silvester).

72 *Ibid.* (Zackary Massingham).

> avons accès à ce genre de choses, que nous pouvons utiliser pour la publicité. Sachez que nous n'avions pas accès au lecteur tout entier[73].

Qui plus est, 625 000 livres (environ 1.1 millions de dollars canadiens) ont été dépensées par Vote Leave au nom de BeLeave par l'entremise d'AIQ, malgré le fait que ses représentants ont déclaré qu'il n'y avait aucune coordination entre les clients de la campagne pour le Brexit. Questionné sur le fait qu'il savait que, si cet argent avait été dépensé par Vote Leave en son nom, cela aurait contrevenu à la législation britannique sur le financement des élections, M. Massingham a répondu : « Oui, cela les aurait mis au-dessus de leur plafond[74]. »

En ce qui concerne la collaboration des représentants d'AIQ avec la commissaire à l'information du Royaume-Uni, M. Silvester a affirmé qu'ils collaborent avec elle depuis que son bureau les a approchés :

> Le 17 mai 2017, la commissaire à l'information du Royaume-Uni nous a envoyé une lettre. Nous avons répondu le 24 mai, puis nous n'avons plus eu de ses nouvelles jusqu'au 30 janvier 2018. Nous avons également répondu à cette nouvelle lettre[75].

Pendant le témoignage des représentants d'AIQ devant le Comité le 24 avril, un membre du Comité a reçu un message provenant du président du comité du Royaume-Uni qui étudie le même dossier, Damian Collins, qui venait tout juste de parler à la commissaire à l'information du Royaume-Uni, Elizabeth Denham. Cette dernière a indiqué à M. Collins qu'AIQ avait refusé de répondre à ses questions précises sur l'utilisation des données pendant la campagne référendaire et qu'elle envisageait de prendre d'autres mesures juridiques pour obtenir l'information dont elle a besoin[76].

Le Comité note qu'AIQ lui a fourni des copies de ses deux lettres envoyées à la commissaire à l'information du Royaume-Uni le 24 mai 2017 et le 5 mars 2018. Dans leur lettre du 5 mars 2018, les représentants d'AIQ indiquent ce qui suit :

> [TRADUCTION] Nous ne sommes pas assujettis à l'autorité de votre commissariat [...] Nous jugeons que notre participation dans l'enquête que mène le commissariat est terminée[77].

---

73 *Ibid.* (Jeff Silvester).

74 *Ibid.*, 1015 (Zackary Massingham).

75 *Ibid.*, 0855 (Jeff Silvester).

76 ETHI, *Témoignages*, 1re session, 42e législature, 24 avril 2018, 1010 (M. Nathaniel Erskine-Smith).

77 Lettre d'AIQ au Commissariat à l'information du Royaume-Uni, 5 mars 2018.

Même s'il est vrai que, techniquement, les représentants d'AIQ ont répondu à la commissaire du Royaume-Uni en lui envoyant deux lettres, force est de constater que la commissaire a jugé que leurs réponses équivalaient à un refus de collaborer avec elle.

Lors de son témoignage devant le Comité, M[me] Denham a rapporté le manque de coopération de la part d'AIQ, notant toutefois des communications récentes entre les parties et la possibilité d'une meilleure collaboration à l'avenir[78].

Le Comité tient à souligner qu'il a totalement confiance en M[me] Denham et qu'il se fie à son jugement. Le Comité note également que M. Silvester a comparu devant le Comité une deuxième fois le 12 juin 2018 pour répondre à de nouvelles questions. En général, il a fait les mêmes affirmations que lors de sa première comparution.

PARTIE 2 : LE POINT DE VUE DE REPRÉSENTANTS D'ORGANISATIONS

A. Mozilla Corporation

Marshall Erwin, directeur de la Fiducie et la Sécurité chez Mozilla, a comparu au nom de Mozilla Corporation. Il a expliqué que le navigateur de Mozilla, Firefox, intègre une série de principes en matière de protection des données qui orientent les pratiques de collecte de données de Mozilla[79]. Selon lui, Mozilla a fait le choix de ne pas collecter les données concernant ses utilisateurs, comme leur historique de navigation. Il a expliqué de la manière suivante comment Mozilla procède :

> Mozilla collecte par défaut un ensemble de données limitées à l'aide du navigateur. Cela nous permet essentiellement de comprendre comment les gens utilisent la technologie. À titre d'exemple, nous collectons des renseignements sur les fonctionnalités du navigateur que les gens utilisent. Cela dit, nous tenons à préciser que cela n'est aucunement lié aux pages Web que les gens consultent[80].

M. Erwin a identifié trois aspects problématiques concernant les mesures de protection de la vie privée prises par les grandes entreprises technologiques :

> Ces paramètres de confidentialité sont souvent cachés et difficiles à trouver. L'industrie ne prend aucune mesure proactive pour aider les gens à comprendre et à utiliser les

78 ETHI, *Témoignages*, 1re session, 42e législature, 24 avril 2018, 1010, 1020 et 1025; ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0905 (Elizabeth Denham, commissaire à l'information, Bureau de la commissaire à l'information du Royaume-Uni).

79 ETHI, *Témoignages*, 1re session, 42e législature, 26 avril 2018, 0955 (Marshall Erwin, directeur, Fiducie et Sécurité, Mozilla Corporation).

80 *Ibid.*

> paramètres de confidentialité. Par conséquent, même si les utilisateurs disposent de moyens techniques pour protéger leurs renseignements personnels, ils n'exercent pas un contrôle significatif à cet égard.
>
> Deuxièmement, les paramètres par défaut de ces contrôles ne sont pas raisonnables et ne correspondent pas aux attentes des utilisateurs quant à ce qui se passe réellement lorsqu'ils utilisent un produit ou un service. Les utilisateurs consentent par défaut à la collecte et à la communication de données délicates, ce qui va à l'encontre de ce que nous appelons le principe des réglages raisonnables à la base même de Firefox. Ces paramètres sont rarement utilisés dans l'industrie actuellement.
>
> Troisièmement, les modalités de la collecte et du partage de données liées à ces paramètres de confidentialité sont toujours larges et permissives. Le principe de la collecte limitée de données de base que nous appliquons chez Mozilla n'est pas une pratique commune dans l'industrie[81].

Selon M. Erwin, ces trois aspects sont en jeu dans les problèmes liés à Facebook et à Cambridge Analytica[82].

En ce qui concerne Facebook, M. Erwin a noté que Mozilla a pris la décision de suspendre ses activités publicitaires sur Facebook lorsque le scandale concernant Cambridge Analytica a éclaté et que ces activités sont toujours suspendues[83]. Il a précisé que ce sont les paramètres par défaut associés aux développeurs tiers qui ont motivé ce choix, parce que ces paramètres étaient inexacts et semblaient transmettre les données aux développeurs en question[84].

M. Erwin a également noté ce qui suit concernant les activités de suivi de Facebook:

> Il y a deux semaines, devant le Congrès américain, Facebook a fait valoir que ses activités de suivi sont en tous points identiques aux activités quotidiennes d'entreprises comme Twitter, Pinterest et Google. C'est tout à fait juste. Il s'agit d'une pratique commune dans l'ensemble de l'industrie; ce n'est absolument pas unique à Facebook[85].

En ce qui concerne la LPRPDE, M. Erwin a formulé la recommandation suivante :

---

81 *Ibid.*

82 *Ibid.*

83 *Ibid.*

84 *Ibid.*, 1025.

85 *Ibid.*, 1000.

> Si le Comité veut vraiment changer les choses, il faudrait miser sur l'application de la loi au Canada. Encore une fois, je crois que la LPRPDE est un bon cadre, auquel on pourra apporter quelques changements, mais il sera utile de renforcer l'application de la loi...[86]

Enfin, M. Erwin s'est prononcé sur l'entrée en vigueur du RGPD dans l'Union européenne de la manière suivante :

> Il y a un grand malaise autour du RGPD. En gros, les entreprises s'inquiètent des redevances de 4 % prévues dans le RGPD. C'est probablement une bonne chose puisque cela forcera les entreprises à s'améliorer. Le problème avec le RGPD pour bon nombre d'entreprises, à mon avis, c'est le manque de clarté au sujet de ce que doivent faire les entreprises pour le respecter et ne pas s'exposer à une amende. Le facteur de motivation associé à cette amende est sain et est utile pour l'industrie[87].

Le Comité note que la recommandation de M. Erwin à l'effet de miser sur une application renforcée de la LPRPDE et son analyse de l'impact du RGPD pour les entreprises – qui sont deux éléments reliés – rejoignent les recommandations faites par le Comité dans son rapport sur l'examen de la LPRPDE publié en février 2018 et réitérées dans le présent rapport.

B. Google

Colin McKay, chef des Politiques publiques et des relations gouvernementales chez Google Canada, a comparu au nom de Google Canada. Il a présenté au Comité les différents outils de Google en matière de protection de la vie privée, comme Mon compte, Security Checkup, Privacy Checkup, Google Takeout et Google Play Protect[88].

En réponse aux questions des membres du Comité et relativement à la recommandation de M. Balsillie de concevoir une stratégie nationale des données (expliquée dans la prochaine partie du présent rapport), M. Mckay y est allé de sa propre recommandation:

> Voilà l'occasion pour le gouvernement de créer une stratégie nuancée qui aide le Canada à se démarquer du reste du monde, non seulement dans le secteur de la technologie, mais également dans celui de la santé, où nous avons déjà une bonne longueur d'avance en ce qui concerne les renseignements médicaux, le secteur de l'agriculture, le secteur des mines et le secteur manufacturier.

---

86 *Ibid.*, 1020.

87 *Ibid.*, 1025.

88 ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0955 (Colin McKay, chef, Politiques publiques et relations gouvernementales, Google Canada).

> Il n'est pas nécessaire qu'une stratégie en matière de données soit aussi restrictive ou prescriptive que l'a laissé entendre M. Balsillie. En fait, une stratégie qui tenterait d'isoler le Canada ou qui créerait des obligations qui ne sont pas semblables à celles qui existent ailleurs dans le monde limiterait les possibilités d'innovation offertes aux Canadiens, et ce, tant au Canada qu'à l'étranger. Tout cadre réglementaire doit être cohérent et prévisible[89].

Il a également précisé que Google ne vend pas les renseignements personnels de ses utilisateurs et que ces renseignements ne sont pas échangés avec les annonceurs[90].

En ce qui concerne l'entrée en vigueur du RGPD, M. McKay a fait l'affirmation suivante :

> Nous investissons dans les équipes et nous améliorons nos outils pour nous conformer au RGPD depuis très longtemps. C'est un défi extrêmement complexe, même pour une entreprise de notre taille. C'est un défi encore plus grand, non seulement pour les petites entreprises, mais aussi pour les commissaires à la protection de la vie privée en Europe.
>
> Ce que nous faisons se reflète dans les outils que j'ai mentionnés dans ma déclaration préliminaire. Cela se reflète dans le genre de permissions et de contrôle que chaque utilisateur a sur tous nos services partout dans le monde.
>
> Les obligations imposées par le RGPD et les attentes concernant la protection des données en Europe trouvent écho dans les services fournis par Google aux utilisateurs du monde entier[91].

Le Comité prend acte de l'importance de l'impact de l'entrée en vigueur du RGPD sur une entreprise de l'ampleur de Google.

C. Conseil des innovateurs canadiens

Jim Balsillie, président du Conseil des innovateurs canadiens, a comparu au nom de ce dernier. Il a présenté au Comité la gestion des données comme étant la plus importante question de politique publique de notre époque[92]. Il a également mentionné que le Conseil des innovateurs canadiens a demandé au gouvernement de concevoir une stratégie nationale des données, « de façon à s'assurer que les flux transfrontaliers de données et d'information servent les intérêts de l'économie canadienne[93]. »

---

89 *Ibid.*, 1010.

90 *Ibid.*

91 *Ibid.*, 1045.

92 *Ibid.*, 1000 (Jim Balsillie, président, Conseil des innovateurs canadiens).

93 *Ibid.*

> Une stratégie nationale en matière de données devrait faire en sorte de systématiser le traitement de la concurrence dans les sections des accords de libre-échange portant sur les données, y compris le droit à un accès concurrentiel aux données qui circulent sur de grandes plateformes et qui possèdent un statut de facto de service public. Si le Canada ne crée pas des lois adéquates sur l'hébergement, la localisation et l'acheminement des données qui protègent les Canadiens, alors nos données sont assujetties aux lois étrangères, ce qui fait du Canada un État client[94].

Selon M^e^ Balsillie, une stratégie nationale de gestion des données devrait également prendre en compte le comportement concurrentiel des entreprises et la question de la propriété des données[95].

En ce qui concerne la situation impliquant Facebook et Cambridge Analytica, M^e^ Balsillie a argué que :

> Le scandale de Cambridge Analytica et de Facebook n'est pas une atteinte à la vie privée ni une question de gouvernance d'entreprise. Ce n'est même pas une question de confiance. C'est une question de modèle d'entreprise fondé sur l'exploitation des lacunes actuelles des lois canadiennes en matière de gouvernance des données[96].

Selon M^e^ Balsillie, Facebook et Google sont des entreprises fondées exclusivement sur le principe de la surveillance de masse et que le « capitalisme de surveillance » constitue actuellement la plus importante force du marché[97].

En ce qui concerne l'entrée en vigueur du RGPD, il a formulé la recommandation suivante : mettre en œuvre des dispositions inspirées du RGPD pour le Canada[98].

> Le RGPD offre de précieuses leçons et constitue un bon point de départ pour les législateurs et les organismes de réglementation du Canada. Il s'agit d'une avancée universellement reconnue en matière de protection de la vie privée et de contrôle des données[99].

Dans cet ordre d'idées, le Comité formule la recommandation suivante :

---

94 Ibid.

95 *Ibid.*, 1045.

96 *Ibid.*, 1000.

97 *Ibid.*

98 *Ibid.*

99 *Ibid.*

Recommandation 2 sur la mise en œuvre au Canada de mesures semblables à celles du *Règlement général sur la protection des données* :

Que le gouvernement du Canada mette immédiatement en œuvre des mesures pour veiller à ce que des protections semblables à celles du *Règlement général sur la protection des données* soient mises en place au Canada, y compris les recommandations contenues dans le rapport sur la *Loi sur la protection des renseignements personnels et les documents électroniques* présenté en février 2018.

En ce qui concerne la question du droit applicable aux données, qui sont constamment en mouvement, M^e^ Balsillie a fourni l'explication suivante :

> un élément très central du RGPD et qui a donné lieu à un énorme bras de fer entre Bruxelles et Washington pendant de nombreuses années, c'est cet élément de sécurité des itinéraires. Il importe de comprendre que, peu importe ce que nous réglementons au Canada, entre 80 et 90 % de nos données passent par les États-Unis, selon ce que m'ont dit des experts. Même si je vous envoie un courriel de l'autre côté de la table, il sera acheminé à l'extérieur. C'est ce qu'on appelle l'effet boomerang. Il faut comprendre que, selon la loi américaine, les données canadiennes n'ont aucun droit aux États-Unis. Vous n'avez aucun droit à la vie privée; vous n'avez aucun droit à quoi que ce soit. L'Union européenne a également géré le routage de façon à ne jamais abandonner la compétence sur le traitement approprié de ces données[100].

À cet égard, le Comité recommande ce qui suit :

Recommandation 3 sur la souveraineté des données :

Que le gouvernement du Canada établisse des règles et des lignes directrices sur la propriété des données et la souveraineté des données afin de mettre un terme à la collecte et à l'utilisation non autorisées des renseignements personnels des citoyens. Ces règles et lignes directrices devraient tenir compte des défis que représente l'infonuagique.

Enfin, M^e^ Balsillie a souligné le fait que la protection de la vie privée et les services numériques – publics et privés – ne sont pas en opposition, en offrant l'exemple de l'Estonie qui « montre qu'une meilleure gouvernance des données entraîne une augmentation de la protection de la vie privée dans les services numériques[101]. »

---

100 *Ibid.*, 1040.

101 *Ibid.*, 1000.

Le Comité prend acte des recommandations de M^e Balsillie et note qu'il continuera d'étudier cet exemple de l'Estonie dans le cadre de son étude sur les conséquences pour la protection des renseignements personnels de la mise en œuvre de services gouvernementaux numériques au Canada.

PARTIE 3 : LE POINT DE VUE DE COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE ET À L'INFORMATION ET D'UNIVERSITAIRES

A. Enquêtes en cours

L'affaire impliquant Cambridge Analytica et Facebook et les révélations de M. Wylie ont suscité non seulement l'attention du commissaire à la protection de la vie privée du Canada[102], mais aussi celle du commissaire à l'information et de la protection de la vie privée de la Colombie-Britannique[103] et de la commissaire à l'information du Royaume-Uni[104].

1. Commissaire à la protection de la vie privée du Canada

Le 20 mars 2018, le Commissariat à la protection de la vie privée du Canada (CPVP) a publié un communiqué de presse dans lequel il annonçait qu'après avoir reçu une plainte contre Facebook concernant le présumé accès non autorisé aux profils d'utilisateurs publiés sur Facebook, il avait lancé une enquête. Le commissaire à la protection de la vie privée, Daniel Therrien, a indiqué que l'enquête permettra d'examiner la conformité de Facebook à la LPRPDE, la loi fédérale qui s'applique aux organismes du secteur privé. Il a aussi révélé que le CPVP restera en contact avec le Bureau de la commissaire à l'information du Royaume-Uni, qui mène une enquête semblable[105].

Le 5 avril 2018, le CPVP a annoncé que son enquête sur Facebook sera menée conjointement avec le Commissariat à l'information et à la protection de la vie privée de la

---

102 Commissariat à la protection de la vie privée du Canada, *Le commissaire à la protection de la vie privée lance une enquête sur Facebook*, communiqué, 20 mars 2018; Commissariat à la protection de la vie privée du Canada, *Les commissariats à la protection de la vie de la Colombie-Britannique et du Canada lancent des enquêtes conjointes sur AggregateIQ et Facebook*, communiqué, 5 avril 2018.

103 Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, *BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook*, communiqué, 5 avril 2018.

104 Royaume-Uni, Bureau de la commissaire à l'information, « ICO statement: investigation into data analytics for political purposes », 2 mai 2018 [TRADUCTION].

105 Commissariat à la protection de la vie privée du Canada, « Le commissaire à la protection de la vie privée lance une enquête sur Facebook », communiqué, 20 mars 2018.

Colombie-Britannique (CIPVP), qui mène également une étude en raison des allégations qui ont été faites à l'égard d'AIQ, puisque l'entreprise est située dans cette province[106].

2. Commissaire à l'information et la protection de la vie privée de la Colombie-Britannique

Le CIPVP a lancé une enquête à l'égard d'AIQ à la fin de l'année 2017[107]. Comme indiqué ci-dessus, celui-ci et le CPVP mènent des enquêtes conjointes sur AIQ et Facebook. Ces enquêtes visent à déterminer si les organismes respectent la LPRPDE et la *Personal Information Protection Act* de la Colombie-Britannique[108].

3. Commissaire à l'information du Royaume-Uni

La commissaire à l'information du Royaume-Uni mène actuellement une enquête sur l'utilisation et l'analyse de données par les responsables de campagnes politiques, les partis politiques, les entreprises de médias sociaux et autres entreprises dans le domaine. Elle fait enquête auprès d'une trentaine d'entreprises, dont Facebook, en vue de déterminer de quelle façon des données ont pu être recueillies au moyen d'une tierce application sur cette plateforme, puis communiquées à Cambridge Analytica. Le Commissariat mène aussi une enquête plus vaste sur l'utilisation des médias sociaux dans les campagnes politiques[109].

B. Commentaires des commissaires à l'égard de leurs pouvoirs d'exécution

Le commissaire à la protection de la vie privée du Canada a comparu devant le Comité le 17 avril 2018. À l'égard de la protection des renseignements personnels et des pouvoirs qu'il possède en vertu de la législation canadienne, M. Therrien a fait les commentaires suivants :

---

106 Commissariat à la protection de la vie privée du Canada, *Les commissariats à la protection de la vie de la Colombie-Britannique et du Canada lancent des enquêtes conjointes sur AggregateIQ et Facebook*, communiqué, 5 avril 2018.

107 *Ibid.*

108 Bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, *BC, federal Privacy Commissioners initiate joint investigations into AggregateIQ, Facebook*, communiqué, 5 avril 2018.

109 Royaume-Uni, Commissariat à l'information, Statement, 2 mai 2018 [TRADUCTION].

> Bien sûr, au Canada, nous avons des lois relatives à la protection de la vie privée. Mais celles-ci sont très permissives et accordent aux entreprises une grande latitude en ce qui concerne l'utilisation des renseignements personnels dans leur propre intérêt. En vertu de la *Loi sur la protection des renseignements personnels et les documents électroniques*, la LPRPDE, les organisations doivent respecter le principe de responsabilité, mais les Canadiens ne peuvent se fier exclusivement aux entreprises pour gérer leurs renseignements de façon responsable. La transparence et la responsabilité sont nécessaires, mais elles ne sont pas suffisantes.
>
> Pour être clair, il ne suffit pas de demander aux entreprises d'être à la hauteur de leurs responsabilités. Les Canadiens ont besoin de lois plus strictes en matière de protection des renseignements personnels qui les protégeront lorsque les organisations échoueront à le faire [...].
>
> Compte tenu de l'opacité des modèles d'affaires et de la complexité des flux de données, la loi devrait permettre au commissariat, à titre de tiers indépendant, de se rendre dans une organisation et de vérifier si cette dernière respecte les principes de protection de la vie privée, et ce, sans devoir au préalable soupçonner qu'il y a eu violation de la loi.
>
> Le moment est aussi venu de conférer au commissariat le pouvoir d'émettre des ordonnances et d'imposer des sanctions pécuniaires contre ceux qui refusent de se conformer à la loi[110].

Le 3 mai 2018, M. Collins a comparu devant le Comité. Il a mentionné que l'une des raisons pour lesquelles son comité appuie l'octroi de pouvoirs additionnels à la commissaire à l'information du Royaume-Uni, dont le pouvoir de rendre visite à certaines compagnies afin de récolter de l'information ou des documents sans donner de préavis, est la difficulté de savoir comment une entreprise respecte, par exemple, le RGPD de l'Union européenne. Il précise :

> Je crois qu'une des grandes questions qui nous ont été posées, c'est comment savoir si une entreprise comme Facebook se conforme aux critères de la RGDP [*sic*]? Et c'est d'ailleurs pour cette raison que nous étions pour l'élargissement des pouvoirs de la commissaire à l'information, afin qu'elle puisse mieux étayer ses enquêtes. Si quelqu'un demande de récupérer ses données ou de les faire détruire, comment savoir que cette requête a été respectée? Si quelqu'un veut récupérer des données qui ont aussi été obtenues par des développeurs de Facebook, qui va régir cela? La meilleure solution, je crois, est de veiller à ce que les autorités aient le pouvoir de faire des inspections impromptues lorsqu'elles soupçonnent une brèche[111].

---

110 ETHI, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0845 (Daniel Therrien, Commissaire à la protection de la vie privée du Canada).

111 ETHI, *Témoignages*, 1re session, 42e législature, 3 mai 2018, 0930 (Damian Collins).

Il a jouté qu'à son avis, il est très important qu'un commissaire à l'information (dans le contexte canadien, un commissaire à la protection de la vie privée) ait l'autorité non seulement de demander la production de documents, mais également le droit d'aller saisir cette information si la compagnie refuse de fournir les documents recherchés, et un pouvoir significatif d'imposer des sanctions[112].

Le 10 mai 2018, le Comité a entendu le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, Michael McEvoy, et la commissaire à l'information du Royaume-Uni, Elizabeth Denham.

En Colombie-Britannique, la LPRPDE est supplantée par la PIPA, car cette loi provinciale a été reconnue comme essentiellement similaire à la législation fédérale. En vertu de la PIPA, le commissaire à l'information et à la protection de la vie privée de cette province possède des pouvoirs d'exécution plus larges que ceux dont dispose le commissaire à la protection de la vie privée du Canada. Il peut par exemple imposer des amendes et émettre des ordonnances. M. McEvoy explique :

> Notre bureau a officiellement signifié qu'il est favorable à ce que le Parlement renforce les pouvoirs du Commissariat à la protection de la vie privée du Canada.
>
> Je pense que nous devons y réfléchir dans l'intérêt des citoyens. Compte tenu des affaires sur lesquelles vous enquêtez, les Canadiens veulent avoir l'assurance qu'une entité investie d'un pouvoir réglementaire veille à leurs intérêts. Cela sera possible que si l'organisme de réglementation détient le pouvoir de s'assurer que les problèmes de ce genre seront corrigés efficacement s'ils suscitent des inquiétudes ou s'il y a transgression de la loi[113].

M[me] Denham dispose aussi, en vertu du *Data Protection Act 1998* (DPA), d'un bien plus grand éventail de pouvoirs d'exécution que le commissaire à la protection de la vie privée du Canada. À l'égard de ces pouvoirs, par contraste avec ceux de son équivalent canadien, elle fait les commentaires suivants :

> [...] je dirais que les pouvoirs du commissaire à la protection de la vie privée du Canada sont moins étendus qu'ailleurs dans le monde. Lorsque nous avons affaire à des entreprises internationales de données et que nous devons faire enquête rapidement, il est très important, à mon avis, d'être en mesure de rendre des ordonnances, d'imposer des pénalités administratives, des amendes et, surtout de saisir du matériel et d'agir rapidement.

---

112 *Ibid.*, 1010.

113 ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0910 (Michael McEvoy, commissaire, Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique).

> Même les pouvoirs que je détiens en vertu de la *Data Protection Act* du Royaume-Uni ne suffisent pas dans ce cas-ci. Le gouvernement a réagi très rapidement et déposé des modifications, qui ont été adoptées hier soir, afin de nous donner des pouvoirs accrus de faire des inspections sans préavis, d'utiliser des mandats simplifiés, de rendre des ordonnances d'urgence et aussi d'infliger des sanctions pénales pour destruction de dossiers et de renseignements.
>
> Dans le contexte général des entreprises numériques, il est important de pouvoir agir rapidement dans l'intérêt public[114].

En vertu de ce qui précède et bien que l'étude du Comité ne soit pas encore terminée, le Comité est d'avis que les recommandations qu'il a faites en février 2018 à l'égard des pouvoirs dont dispose le commissaire à la protection de la vie privée du Canada dans son rapport intitulé « Vers la protection de la vie privée dès la conception : examen de la *Loi sur la protection des renseignements personnels et les documents électroniques* » (le « Rapport sur la LPRPDE ») [115] ont pris encore plus d'importance. En raison des récents développements en matière d'atteinte à la sécurité des renseignements personnels des citoyens en ligne sur la scène internationale, ces recommandations ont même pris un certain air d'urgence.

Le Comité est d'avis qu'accorder davantage de pouvoirs au commissaire est impératif afin d'assurer la protection des renseignements personnels des citoyens canadiens. Il réitère donc les recommandations suivantes tirées de son Rapport sur la LPRPDE :

Recommandation 4 sur les pouvoirs d'exécution du commissaire à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir de rendre des ordonnances et le pouvoir d'imposer des amendes en cas de non-respect de ces ordonnances[116].

---

114 *Ibid.*, 0910 (Elizabeth Denham).

115 ETHI, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, douzième rapport, 1re session, 42e législature, février 2018, recommandations 15 et 16.

116 Cette recommandation est la même que la Recommandation 15 dans : ETHI, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, douzième rapport, 1re session, 42e législature, février 2018, p. 69.

Recommandation 5 sur les pouvoirs du commissaire à la protection de la vie privée en matière d'audit :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs étendus en matière d'audit, incluant le pouvoir de choisir les plaintes sur lesquelles enquêter[117].

Comme mentionné ci-dessus, M[me] Denham a indiqué que malgré tous les pouvoirs dont elle dispose en vertu de la loi au Royaume-Uni, elle a tout de même eu des difficultés dans le cadre de son enquête, par exemple à l'égard du mandat de perquisition qu'elle voulait obtenir afin de saisir des documents dans les bureaux de Cambridge Analytica et pour lequel elle a dû attendre plusieurs jours. Elle a indiqué :

> [...] je conviens avec vous que les dispositions actuelles de la loi ne nous permettent pas de procéder rapidement avec un mandat. Nous devons être en mesure de traiter les cas de cybercriminalité et tout autre délit lié aux données. Les modifications que le gouvernement vient d'apporter à la loi nous conféreront de nouveaux pouvoirs qui nous permettront de réagir plus rapidement, sans être obligés de donner des préavis longtemps d'avance aux organisations. Cela dit, nous avons réussi à saisir de grandes quantités de données chez Cambridge Analytica et nous avons exécuté deux autres mandats dans le cadre de cette enquête. Nous avons donc beaucoup d'information en main. S'il existe des liens entre une compagnie et une autre et si leur propriété intellectuelle et leurs données sont utilisées par une nouvelle compagnie, nous pourrons alors faire enquête et poursuivre nos travaux. Si une compagnie déclare faillite, comme dans ce cas-ci, nous restons en contact avec les administrateurs et nous pouvons prendre des mesures d'exécution, tant au criminel qu'au civil[118].

M. Collins a indiqué ce qui suit à l'égard des nouveaux pouvoirs de la commissaire à l'information du Royaume-Uni :

> Le gouvernement semble déjà vouloir accéder à une de nos demandes, à savoir l'octroi de pouvoirs supplémentaires à la commissaire à l'information pour lui permettre de prendre et de saisir des données sans préavis, afin d'éviter d'attendre de nouveau cinq jours avant d'obtenir un mandat de perquisition, comme dans le cas de Cambridge Analytica, ce qui était ridicule. Elle aura des pouvoirs accrus qui l'aideront à conclure cette enquête et celles qui suivront[119].

---

117 Cette recommandation est la même que la Recommandation 16 dans : ETHI, *Vers la protection de la vie privée dès la conception : Examen de la Loi sur la protection des renseignements personnels et les documents électroniques*, douzième rapport, 1re session, 42e législature, février 2018, p. 70.

118 ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0905 (Elizabeth Denham).

119 ETHI, *Témoignages*, 1re session, 42e législature, 3 mai 2018, 0900 (Damian Collins).

Le Comité est d'avis que de tels pouvoirs devraient également faire l'objet d'une modification de la LPRPDE et, en plus des pouvoirs recommandés ci-dessus, recommande ce qui suit :

Recommandation 6 sur des pouvoirs d'exécution additionnels du commissaire à la protection de la vie privée :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'accorder au commissaire à la protection de la vie privée des pouvoirs d'exécution, incluant le pouvoir d'émettre des avis urgents à une organisation relativement à la production de documents pertinents dans une durée plus courte et le pouvoir de saisir des documents dans le cadre d'une enquête, sans préavis.

Enfin, M. Therrien a mentionné que bien qu'il ait une grande latitude en matière de coopération avec les organismes de régulation relatifs à la protection des renseignements personnels d'autres juridictions, rien dans la loi ne lui permet de partager de l'information avec d'autres organismes de régulation, comme par exemple le Bureau de la concurrence du Canada. Les enquêtes du CPVP relatives à la LPRPDE peuvent impliquer des questions qui touchent à la fois le droit à la protection de la vie privée et le droit de la concurrence. Selon lui, le fait que le CPVP ne puisse pas partager de l'information avec certains autres organismes de régulation est une lacune du régime législatif[120].

Le Comité est d'accord avec M. Therrien et recommande :

Recommandation 7 sur le partage d'information entre le commissaire à la protection de la vie privée et d'autres organismes de régulation :

Que la *Loi sur la protection des renseignements personnels et les documents électroniques* soit modifiée afin d'autoriser le commissaire à la protection de la vie privée à partager certaines informations pertinentes dans le cadre d'enquêtes avec le Bureau de la concurrence, d'autres organismes de régulation canadiens et des organismes de régulation à l'échelle internationale, lorsque cela est approprié.

120 ETHI, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0925 et 0930 (Daniel Therrien).

C. Application de la législation en matière de protection de la vie privée aux activités politiques

Le gouvernement du Canada a récemment déposé son projet de loi C-76, la *Loi sur la modernisation des élections*, qui vise à modifier la *Loi électorale du Canada*[121]. Le projet de loi prévoit entre autres l'ajout de dispositions relatives à la protection des renseignements personnels. Ces changements visent surtout à rendre obligatoire, pour les partis politiques au Canada, l'adoption et le maintien d'une politique relative à la protection des données et l'affichage de cette politique en ligne[122].

En vertu du projet de loi, un parti qui contrevient aux dispositions relatives à la protection des renseignements personnels pourrait ne pas être en mesure de devenir un parti enregistré ou perdre le droit d'être enregistré. Les changements proposés ne font par contre pas en sorte que les partis politiques soient sujets à une quelconque loi relative à la protection des renseignements personnels.

M. Therrien a soulevé les lacunes liées à l'absence d'application des lois relatives à la protection de la vie privée aux partis politiques. Il a fait les commentaires suivants:

> Il est également temps d'agir dans le domaine des mesures de protection de la vie privée et des partis politiques.
>
> Comme vous le savez, aucune loi fédérale sur la protection de la vie privée ne s'applique aux partis politiques. La Colombie-Britannique est la seule province qui possède une législation en la matière.
>
> La situation est différente dans de nombreux autres pays. Le Royaume-Uni, la plupart des pays membres de l'Union européenne et la Nouvelle-Zélande, entre autres, ont des lois qui régissent les organisations politiques à cet égard.
>
> En fait, dans de nombreux États membres de l'Union européenne, les renseignements relatifs aux opinions politiques sont considérés comme étant de nature très délicate et, à ce titre, ces renseignements sont considérés comme nécessitant des mesures de protection supplémentaires.
>
> Dans l'environnement numérique, il existe maintenant de nombreux acteurs qui jouent un rôle dans ce domaine, dont les courtiers en données, les entreprises d'analyse de données, les réseaux sociaux, les fournisseurs de contenu, les spécialistes du marketing numérique et les entreprises de télécommunications.

---

121 Chambre des Communes du Canada, Projet de Loi C-76, ***Loi modifiant la Loi électorale du Canada et d'autres lois et apportant des modifications corrélatives à d'autres textes législatifs***.

122 Institutions démocratiques, Document d'information, *Donner aux partis politiques les moyens de mieux protéger la vie privée des Canadiennes et des Canadiens*, 30 avril 2018.

> Par conséquent, pendant que je mène une enquête sur des organisations commerciales comme Facebook et AggregateIQ, je ne suis pas en mesure d'enquêter sur la façon dont les organisations politiques utilisent les renseignements personnels que des entreprises leur transmettent.
>
> Il s'agit, selon moi, d'une lacune importante[123].

M. Therrien a aussi mentionné que l'adoption d'une politique relative à la protection des renseignements personnels n'est pas suffisante. Il a expliqué que :

> Dans la situation actuelle, la plupart des partis politiques fédéraux ont des politiques en matière de protection des renseignements personnels – des codes de déontologie internes, pour ainsi dire, qui régissent leur relation avec les personnes avec lesquelles ils interagissent et au sujet desquelles ils recueillent des renseignements. C'est un début.
>
> Premièrement, si j'en juge par ce que nous avons vu, je pense que la teneur de ces politiques pourrait être rehaussée. Un élément commun qui manque aux politiques en matière de protection des renseignements personnels est le droit des électeurs d'avoir accès aux renseignements personnels qui leur appartiennent et que détiennent les partis politiques fédéraux. C'est une énorme lacune. Il y a, ensuite, la question de la teneur. Cependant, il s'agit de codes volontaires, et aucune personne indépendante des partis ne vérifie si les partis honorent réellement la promesse qu'ils font dans ces politiques. Cela m'amène à la raison très importante pour laquelle les partis politiques devraient être gouvernés par une loi: pour veiller à ce que les règles de droit substantielles, quelles qu'elles soient et qui seront – espérons-le – meilleures que celles qui existent, soient vérifiées par un tiers indépendant[124].

Il a décrit la zone grise dans laquelle se trouvent les partis politiques :

> Par ailleurs, quand j'ai parlé d'une zone grise, c'était dans le sens où, n'ayant pas compétence pour vérifier comment les partis utilisent les renseignements, je ne sais pas ce qui se passe. Les partis se dotent de politiques de protection de la vie privée afin d'assurer un minimum de règles dans leurs relations avec les électeurs. Cependant, ni moi ni aucune autre personne indépendante ne peut vérifier ce qui se passe. Alors, c'est ce que je voulais dire par « zone grise », une zone où il n'y a pas d'arbitre indépendant qui peut s'assurer que les règles qui sont mises en place sont respectées[125].

Le 26 avril 2016, le Comité a entendu les témoignages de Colin Bennett, professeur au Département de science politique de l'Université de Victoria et de Thierry Giasson, professeur titulaire au Département de science politique de l'Université Laval et directeur du Groupe de recherche en communication politique de cette même

---

123 *Ibid.*, 0850.

124 ETHI, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0915 (Daniel Therrien).

125 *Ibid.*, 0940.

institution. Tous deux ont exprimé l'opinion que les partis politiques devraient être sujets à l'application de la législation relative à la protection des renseignements personnels. M. Bennett a indiqué :

> Mon deuxième point est qu'il y a un besoin pressant d'assujettir les partis politiques à la législation canadienne en matière de protection de la vie privée [...] L'une des meilleures façons d'empêcher ce type d'abus que nous voyons à l'étranger est de fixer des règles claires et uniformes quant aux catégories de données auxquelles peuvent avoir recours les partis politiques dans le cadre de leur campagne électorale. Il faut établir des règles du jeu équitables qui interdiraient aux sociétés comme Cambridge Analytica de reproduire au Canada leurs pratiques telles que celles observées ailleurs.
>
> Le Canada est l'un des seuls pays démocratiques avancés dont la législation en matière de protection de la vie privée ne vise pas les partis politiques. La majorité ne sont pas régis par la LPRPDE. Comme il ne s'agit pas d'organismes gouvernementaux, ils ne sont pas régis par la *Loi sur la protection des renseignements personnels*. Ils sont également en grande partie exemptés de l'application de la nouvelle loi antipourriel et de nombreux règlements concernant les abonnés exclus administrés par le CRTC. Il y a bien quelques règles afférentes à la protection de la vie privée et de la sécurité dans la *Loi électorale du Canada*, mais elles ne s'appliquent qu'aux listes d'électeurs et sont sans effet sur les autres sources de renseignements personnels.
>
> Par conséquent, en ce qui concerne les partis politiques, les Canadiens n'ont pas les droits légaux qu'ils ont en ce qui concerne les organismes gouvernementaux et les activités commerciales[126].

Selon M. Bennett, il ne fait aucun doute que le statut quo est inacceptable, puisque le recours aux données personnelles dans le cadre d'élections ne fera qu'augmenter d'ici aux élections fédérales de 2019, particulièrement en ce qui a trait au ciblage politique sur Facebook[127]. M. Giasson a fait écho aux propos de M. Bennett en indiquant que, malgré l'intérêt croissant des médias à l'égard de l'utilisation de données personnelles et d'algorithmes dans le cadre de campagne électorales, « tout ce qui se passe [...] se fait largement à l'insu des Canadiens et dans un contexte où les Canadiens ignorent tout de l'étendue et de l'utilisation que font les partis de leurs données privées »[128]. Il estime que cette réalité a un impact sur la démocratie au Canada. Il renchérit :

> La question fondamentale qui est au cœur du débat que nous tenons en ce moment, c'est qu'il n'y a pas de transparence. Les gens ne savent pas ce que font les partis. Le fait que les partis effectuent un ciblage n'est pas forcément un énorme problème.

---

126 ETHI, *Témoignages*, 1re session, 42e législature, 26 avril 2018, 0845 et 0850 (Colin Bennett, professeur, Département de science politique, University of Victoria).

127 *Ibid.*, 0850.

128 *Ibid.*, 0905 (Thierry Giasson, professeur titulaire, Département de science politique, Université Laval).

> Cependant, le fait que les citoyens ne savent pas ce que font les partis avec les données qu'ils recueillent est un problème, et c'est le problème fondamental. Les partis doivent s'assurer que lorsque les citoyens donnent l'accès à toute forme de donnée qui pourrait être utilisée à des fins de ciblage politique, ils doivent en être informés[129].

De l'avis de M. Bennett, les 10 principes sur lesquels repose la LPRPDE devraient être respectés par les partis politiques. Il recommande également l'adoption d'une certaine mesure d'uniformité dans les pratiques relatives à la protection des renseignements personnels des partis politiques[130]. M. Bennett a aussi noté le dilemme créé par le fait que d'un côté, le directeur général des élections a une connaissance des partis politiques et des principes qui s'appliquent à eux, mais il n'a pas l'expertise ni les ressources nécessaires pour traiter de questions relatives à la protection de la vie privée; de l'autre côté, le CPVP a les compétences et les ressources pour traiter des questions relatives à la protection des renseignements personnels, mais il n'a pas le mandat législatif de le faire lorsque ces questions visent les partis politiques[131].

M. McEvoy a expliqué au Comité que la Colombie-Britannique est la seule province où les partis politiques sont sujets aux obligations prévues sous une loi visant la protection des renseignements personnels, la PIPA. Il a fait les commentaires suivants à l'égard de l'impact de l'adoption d'une telle mesure législative dans sa province :

> Les partis politiques de ma province sont assujettis à la PIPA depuis son adoption en 2004. Au cours des 14 années écoulées depuis son adoption, je peux vous assurer que la démocratie a continué de prospérer sans entrave en Colombie-Britannique. Nous n'avons été informés d'aucune préoccupation ou suggestion laissant entendre que les lois protégeant les renseignements personnels des électeurs limitent la capacité des partis politiques ou des candidats d'atteindre les électeurs.
>
> Les partis politiques de la Colombie-Britannique peuvent recueillir des renseignements personnels sur les électeurs, et ils le font, mais en ayant les mêmes responsabilités et obligations juridiques raisonnables qui s'appliquent aux autres organismes.
>
> En règle générale, cela signifie que les partis politiques obtiennent des renseignements avec le consentement des électeurs, accompagnés d'une explication claire de la façon dont ces renseignements seront utilisés et de la raison pour laquelle ils le seront [...].
>
> La PIPA donne également aux citoyens le droit légal de connaître et de corriger les renseignements personnels que les partis politiques recueillent auprès d'eux et de déposer une plainte au besoin. Ces plaintes sont traitées par mon bureau. Le droit des citoyens d'exercer un contrôle sur leurs renseignements personnels est un principe

---

129 *Ibid.*, 0910.

130 *Ibid.*, 0920 et 0930 (Colin Bennett).

131 *Ibid.*, 0925.

> fondamental de la loi sur la protection des renseignements personnels. Il s'agit d'un principe renforcé par le Règlement général sur la protection des données de l'Union européenne, dont la commissaire Denham vient de parler [...][132].

M. McEvoy a également fourni un exemple de cas où l'habileté du commissaire à l'information et la protection de la vie privée en Colombie-Britannique de faire enquête sur la collecte de renseignements personnels de partis politiques s'est avérée très utile :

> En Colombie-Britannique, nous avons eu l'occasion d'enquêter sur des cas où la collecte de renseignements par le parti au pouvoir a donné lieu à des allégations selon lesquelles le parti aurait franchi une ligne, ou se serait retrouvé dans une zone grise, et qu'il aurait prétendument transféré ces renseignements à des sources du parti.
>
> Si nous n'avions pas eu le pouvoir d'enquêter sur les partis, l'enquête se serait terminée là. Je pense que cela aurait été non seulement problématique pour notre propre enquête, mais aussi parce que le public n'aurait jamais su ce qui est vraiment arrivé aux renseignements recueillis. Comme la loi nous permet d'enquêter sur les partis politiques, nous avons pu effectuer un examen global et en arriver à des conclusions quant à ce qui a pu arriver à ces renseignements. Je crois que cela a renforcé la confiance du public dans le fait que les renseignements ont été traités de manière appropriée. Si cela n'avait pas été le cas, notre bureau aurait pu imposer des sanctions[133].

À l'égard du projet de loi C-76 visant la modification de la *Loi électorale du Canada*, M. McEvoy indique :

> Bien entendu, je sais que les modifications proposées récemment à la *Loi électorale du Canada* obligeront les partis politiques à adopter une politique de protection des renseignements personnels et à la fournir au directeur général des élections. Ces propositions ne sont qu'un petit pas en avant. Elles sont une tentative d'inclusion du principe de la transparence, mais ce n'est là qu'un élément d'un régime adéquat de protection des données[134].
>
> Les modifications proposées n'obligent pas les partis à répondre à la demande d'un électeur pour obtenir l'information qu'ils détiennent à son sujet et elles ne lui donnent pas non plus le droit de demander à un parti de corriger des renseignements inexacts à son sujet. Ce qui est peut-être le plus important, c'est qu'il n'y a aucune disposition permettant à un tiers impartial d'entendre et de trancher une plainte d'un électeur. Ces normes juridiques fondamentales font partie du droit de la Colombie-Britannique depuis des années et sont la norme dans de nombreuses démocraties occidentales. Les partis politiques ne devraient reculer devant aucune de ces obligations juridiques. En fait, leur

---

132 ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0910 (Michael McEvoy).

133 *Ibid.*, 0920.

134 *Ibid.*, 0900.

> mise en œuvre ne fera qu'accroître la confiance des citoyens dans leurs institutions démocratiques[135].

M^me^ Denham a témoigné du fait qu'au Royaume-Uni, les partis politiques sont également sujets à la législation relative à la protection de la vie privée. Elle a indiqué que :

> Au Royaume-Uni, comme dans l'ensemble de l'Union européenne, l'information sur les opinions politiques des particuliers est considérée comme une catégorie de données personnelles particulièrement sensibles à laquelle des mesures de protection supplémentaires s'appliquent en vertu des lois sur la protection des données. Cela signifie donc que les partis et les campagnes politiques sont régis par un ensemble de mesures légales visant la protection des données, le marketing direct et les élections lorsqu'ils traitent des données à des fins électorales, le tout sous la surveillance de mon bureau et de la commission électorale. Cela a toujours été le cas depuis l'adoption de la loi sur la protection des données il y a plus de 20 ans, et c'est simplement admis comme une norme culturelle.
>
> Ces règles sont en place pour assurer la tenue d'élections libres et justes et elles n'entravent pas l'engagement démocratique au Royaume-Uni, mais obligent plutôt les partis politiques à communiquer avec les électeurs d'une manière qui y soit conforme. Vu la place spéciale des partis politiques dans une société démocratique, ils ont obtenu un statut particulier aux termes de la loi britannique sur la protection des données qui leur permet de mener leurs activités de campagne.
>
> Dans mon rôle de traitement des plaintes, j'examine les plaintes formulées à l'endroit des partis politiques par les particuliers qui pensent que leurs données ont été utilisées à mauvais escient. Le nombre de plaintes n'a jamais été particulièrement élevé. Mis à part un pic au moment des élections, les partis politiques n'ont pas été, dans l'ensemble, à l'origine d'une forte proportion des plaintes. Mon bureau a maintenu un dialogue continu avec les partis, les a rencontrés régulièrement et leur a donné des directives sur la façon de se conformer à la loi lorsqu'ils font campagne[136].

M. Wylie a de son côté fait part au Comité de quelques réserves à l'égard de l'application de lois relatives à la protection des renseignements personnels aux partis politiques, indiquant qu'il ne faudrait pas qu'une loi en matière de protection de la vie privée applicable aux partis politiques soit trop restrictive, puisque cela pourrait avoir un impact négatif plutôt que positif sur la démocratie. Il souligne que si les règles imposées empêchent les partis de communiquer avec certaines personnes et isolent une partie de

---

135 *Ibid.*, 0905.

136 *Ibid.*, 0845 (Elizabeth Denham).

la population du discours politique, les discussions stimulantes que le processus démocratique suscite pourraient ne pas avoir lieu[137].

À la lumière des témoignages entendus, le Comité est d'avis que la confiance des citoyens Canadiens serait renforcée s'ils savaient que leurs partis politiques ne sont pas exemptés de l'application de toute loi relative à la protection des renseignements personnels et qu'ils ont des responsabilités prévues par une loi à cet égard, similaires à celles imposées aux organisations des secteurs public et privé en vertu de la *Loi sur la protection des renseignements personnels* et de la LPRPDE. Toute modification législative devrait évidemment tenir compte de la nature particulière des activités des partis politiques, de sorte à ne pas empêcher entièrement l'utilisation de renseignements personnels, mais plutôt à encadrer davantage sa collecte et son utilisation et la transparence qui entoure la gestion de tels renseignements.

Par conséquent, le Comité recommande :

Recommandation 8 sur l'application des lois relatives à la protection de la vie privée aux activités politiques :

Que le gouvernement du Canada prenne certaines mesures afin d'assurer l'application de la législation en matière de protection de la vie privée aux activités politiques, soit par la modification des lois existantes ou par l'adoption d'une nouvelle loi.

CONCLUSION

Comme l'a souligné le commissaire Therrien, « L'intégrité de nos processus démocratiques et la confiance à l'égard de l'économie numérique sont exposées à des risques importants[138]. » D'autres témoins ont souligné les mêmes risques[139]. Alors que les révélations à l'égard de Cambridge Analytica et de Facebook ont exposé les risques liés à la collecte malveillante de renseignements personnels, le Comité est également conscient du fait qu'il y a probablement d'autres organisations qui se prêtent à de telles activités. Les recommandations formulées par le Comité dans ce rapport provisoire sont un pas vers une meilleure protection des renseignements personnels des citoyens Canadiens.

---

137 ETHI, *Témoignages*, 1re session, 42e législature, 29 mai 2018, 1055 (Christopher Wylie).

138 ETHI, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0850 (Daniel Therrien).

139 *Ibid.* (Chris Vickery); ETHI, *Témoignages*, 1re session, 42e législature, 26 avril 2018, 1000 (Marshall Erwin); ETHI, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 1005 (Jim Balsillie).

Bien que la LPRPDE bénéficie actuellement d'un statut d'adéquation par rapport au RGPD, le Comité encourage très fortement le gouvernement du Canada à mettre en œuvre les recommandations qu'il a faites dans son rapport sur la LRPPDE ainsi que les recommandations préliminaires qu'il fait dans le présent rapport. Ces recommandations amélioreraient la protection de la vie privée au Canada et harmoniseraient davantage la législation canadienne avec le RGPD. On ne peut trop insister sur l'urgence de la situation.

Le Comité a l'intention de poursuivre son étude et sa collaboration avec les parlementaires et les autorités réglementaires du Royaume-Uni et des États-Unis afin d'identifier l'éventail des moyens à sa disposition pour atténuer les risques auxquels nos processus démocratiques et notre économie numérique font face. Le Comité formulera d'autres recommandations dans son rapport final, lorsqu'il aura complété son étude.

ANNEXE A
LISTE DES TÉMOINS

Organismes et individus	Date	Réunion
À titre personnel	2018/04/17	99
Chris Vickery, directeur de la recherche sur les risques cybernétiques UpGuard		
Commissariat à la protection de la vie privée du Canada		
Daniel Therrien, commissaire à la protection de la vie privée du canada		
Barbara Bucknell, directrice Politiques, affaires parlementaire et recherche		
Facebook Inc.	2018/04/19	100
Kevin Chan, directeur mondial et chef de la politique publique Facebook Canada		
Robert Sherman, directeur adjoint de la protection des renseignements personnels		
AggregateIQ	2018/04/24	101
Zackary Massingham, directeur général		
Jeff Silvester, chef des opérations		
À titre personnel	2018/04/26	102
Colin J. Bennett, professeur Département de science politique, University of Victoria		
Thierry Giasson, professeur titulaire Département de science politique, Université Laval		
Mozilla Corporation		
Marshall Erwin, directeur Fiducie et Sécurité		
Chambre des communes du Royaume-Uni, Comité spécial sur le numérique, la culture, les médias et le sport	2018/05/03	104
Damian Collins, président, député		
Bureau de la commissaire à l'information du Royaume-Uni	2018/05/10	106
Elizabeth Denham, commissaire à l'information		

Organismes et individus	Date	Réunion
Bureau du Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique		
Michael McEvoy, commissaire		
Conseil des innovateurs canadiens	2018/05/10	106
Jim Balsillie, président		
Google Canada		
Colin McKay, chef, politiques publiques et relations gouvernementales		
Chambre des communes	2018/05/24	108
André Gagnon, sous-greffier, procédure Chambre des communes		
Wendy Gordon, directrice, affaires législatives Bureau du légiste et conseiller parlementaire		
Stéphane am Rhyn, avocat Bureau du légiste et conseiller parlementaire		
À titre personnel	2018/05/29	109
Christopher Wylie		
Commissariat à la protection de la vie privée du Canada	2018/05/31	110
Daniel Therrien, commissaire à la protection de la vie privée du canada		
Barbara Bucknell, directrice Politiques, affaires parlementaire et recherche		
Brent Homan, directeur exécutif Direction de la conformité de la Loi sur la protection des renseignements personnels et les documents électroniques		
Sarah Speevak, conseillère juridique		
À titre personnel	2018/06/07	112
Chris Vickery, directeur de la recherche sur les risques cybernétiques UpGuard		
AggregateIQ	2018/06/12	113
Jeff Silvester, chef des opérations		

ANNEXE B
LISTE DES MÉMOIRES

Organismes et individus

Eatz, Sydney

PROCÈS-VERBAUX

Un exemplaire des *procès-verbaux* pertinents (réunions nos 99, 100 à 102, 104, 106, 108 à 114) est déposé.

Respectueusement soumis,

Le président,
Bob Zimmer

Opinion dissidente du Nouveau parti démocratique et du parti conservateur

Atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook

I. Introduction

Au cours de l'enquête du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique au sujet de l'atteinte à la sécurité des renseignements personnels associée à Cambridge Analytica et Facebook, le Comité a eu un témoignage de Jeff Silvester et Zack Massingham de AggregateIQ (AIQ), une société de conseil politique basée à Victoria. C.-B.

C'était l'opinion unanime du Comité que ce témoignage a été contredit par le témoignage d'autres témoins.

M. Massingham, à l'occasion de son témoignage, a donné l'impression au Comité qu'il n'a pas partagé toutes les données exigées par le Comité, et donc le Comité lui a émis une assignation à comparaitre.

L'assignation étant émise, M. Massingham ne s'est pas présenté, qui soulève des questions sérieuses à propos du pouvoir des comités parlementaires de rendre leur travail de la part du Parlement et le peuple du Canada sans obstruction.

II. Contexte

Au cours de la collecte de preuves et témoignages de cette étude, des allégations préoccupantes ont été faites à propos du rôle qu'a joué AIQ dans des procès démocratiques à travers le monde. Nous avons entendu des témoignages en contradiction directs avec ce que nous ont dit MM. Silvester et Massingham.

Il n'est pas le rôle d'un comité de trouver faute avec des individus, mais de donner au Parlement une analyse claire des faits et des recommandations pour faire des changements législatifs. Pour cela, notre comité a émis des assignations à M. Massingham pour lui donner l'occasion de clarifier leurs témoignages originaux et répondre aux autres témoins.

En correspondance avec le conseil de M. Massingham à propos d'une session de témoignage possible pour le 12 juin, 2018, le Comité a reçu des preuves qu'il n'était pas capable d'apparaitre devant le Comité.

Le Comité a décidé de façon unanime que les preuves présentées n'étaient pas suffisantes pour annuler l'assignation pour le 12 juin, et nous nous attendions qu'il allât apparaitre ce jour-là.

Le 12 juin, M. Massingham ne s'est pas présenté devant le Comité. Aucune explication ne nous était envoyée.

III. Conclusion et recommandations

Les membres néodémocrates et conservateurs du Comité croient que le refus d'apparaitre de M. Massingham est un obstacle au pouvoir du Comité de trouver des faits et de rapporter nos conclusions à la Chambre des Communes.

Dans l'opinion des membres néodémocrates et conservateurs du Comité, laisser passer les actions de M. Massingham créera un précédent qui pourrait compromettre le pouvoir d'autre députés et comités de recueillir des témoignages des témoins sur des sujets d'importance nationale.

Nous croyons que le Comité et son président ont agi comme il se doit au cours de ce procès envers M. Massingham et nous avons essayé d'assurer que le Comité respecte son mandat et ses limites. Mais un témoin qui refuse l'assignation d'un comité requiert une directive de la Chambre des Communes.

Les questions de privilège doivent être soulevées aussi tôt que possible dès qu'ils surviennent pour être recevables. Les membres néodémocrates et conservateurs croient fortement que ce refus de répondre à une assignation par un comité représente une brèche *prima facie* de privilège parlementaire.

Les membres recommandent que le président du Comité soit dirigé à soulever la brèche dans la Chambre des Communes aussi tôt que possible pour une décision du Président de la Chambre des Communes.